Additive Polynomials and Their Role in the Model Theory of Valued Fields*

Franz-Viktor Kuhlmann

Dedicated to Mahmood Khoshkam († October 13, 2003)

8. 7. 2005

Abstract

We discuss the role of additive polynomials and p-polynomials in the theory of valued fields of positive characteristic and in their model theory. We outline the basic properties of rings of additive polynomials and discuss properties of valued fields of positive characteristic as modules over such rings. We prove the existence of Frobenius-closed bases of algebraic function fields $F|K$ in one variable and deduce that F/K is a free module over the ring of additive polynomials with coefficients in K. Finally, we prove that every minimal purely wild extension of a henselian valued field is generated by a p-polynomial.

1 Introduction

This paper is to some extent a continuation of my introductive and programmatic paper [Ku3]. In that paper I pointed out that the ramification theoretical *defect* of finite extensions of valued fields is responsible for the problems we have when we deal with the model theory of valued fields, or try to prove local uniformization in positive characteristic.

In the present paper I will discuss the connection between the defect and additive polynomials. I will state and prove basic facts about additive polynomials and then treat

*This paper was written while I was a guest of the Equipe Géométrie et Dynamique, Institut Mathématiques de Jussieu, Paris, and of the Equipe Algèbre–Géométrie at the University of Versailles. I gratefully acknowledge their hospitality and support. I was also partially supported by a Canadian NSERC grant and by a sabbatical grant from the University of Saskatchewan. Furthermore I am endebted to the organizers of the conference in Teheran and the members of the IPM and all our friends in Iran for their hospitality and support. I also thank Peter Roquette, Florian Pop and Philip Rothmaler for their helpful suggestions and inspiring discussions, and the two referees for their careful reading of the paper, their corrections and numerous useful suggestions. The final revision of this paper was done during my stay at the Newton Institute at Cambridge; I gratefully acknowledge its support.

several instances where they enter the theory of valued fields in an essential way that is particularly interesting for model theorists and algebraic geometers. I will show that non-commutative structures (skew polynomial rings) play an essential role in the structure theory of valued fields in positive characteristic. Further, I will state the main open questions. I will also include some exercises.

In the next section, I will give an introduction to additive polynomials and describe the reasons for their importance in the model theory of valued fields. For the convenience of the reader, I outline the characterizations of additive polynomials in Section 3 and the basic properties of rings of additive polynomials in Section 4. For more information on additive polynomials, the reader may consult [Go]. The remaining sections of this paper will then be devoted to the proofs of some of the main theorems stated in Section 2.

2 Reasons for the importance of additive polynomials in the model theory of valued fields

A polynomial $f \in K[X]$ is called **additive** if

$$f(a+b) \;=\; f(a) + f(b) \tag{1}$$

for all elements a, b in every extension field L of K, that is, if the mapping induced by f on L is an endomorphism of the additive group $(L, +)$. If K is infinite, then f is additive already when condition (1) is satisfied for all $a, b \in K$: see part b) of Corollary 23 in Section 3.

It follows from the definition that an additive polynomial cannot have a non-zero constant term. If the characteristic $\operatorname{char} K$ is zero, then the only additive polynomials over K are of the form cX with $c \in K$. If $\operatorname{char} K = p > 0$, then the mapping $a \mapsto a^p$ is an endomorphism of K, called the **Frobenius**. Therefore, the polynomial X^p is additive over any field of characteristic p. Another famous and important additive polynomial is $\wp(X) := X^p - X$, the additive **Artin-Schreier polynomial**. An extension of a field K of characteristic p generated by a root of a polynomial of the form $X^p - X - c$ with $c \in K$ is called an **Artin-Schreier extension**. We will see later that Artin-Schreier extensions play an important role in the theory of fields in characteristic p.

Note that there are polynomials defined over a finite field which are not additive, but satisfy the condition for all elements coming from that field. For example, we know that $a^p = a$ and thus $a^{p+1} - a^2 = 0$ for all $a \in \mathbb{F}_p$. Hence, the polynomial $g(X) := X^{p+1} - X^2$ satisfies $g(a+b) = 0 = g(a) + g(b)$ for all $a, b \in \mathbb{F}_p$. But it is not an additive polynomial. To show this, let us take an element ϑ in the algebraic closure of $\mathbb{F}_p$ such that $\vartheta^p - \vartheta = 1$. Then $g(\vartheta) = \vartheta(\vartheta^p - \vartheta) = \vartheta$. On the other hand, $g(\vartheta+1) = (\vartheta+1)((\vartheta+1)^p - (\vartheta+1)) = (\vartheta+1)(\vartheta^p + 1^p - \vartheta - 1) = \vartheta + 1 \neq \vartheta = g(\vartheta) + g(1)$. Hence, already on the extension field $\mathbb{F}_p(\vartheta)$, the polynomial g does not satisfy the additivity condition.

The following well known theorem gives a very useful characterization of additive polynomials. I will present a proof in Section 3.

Theorem 1 *Let p be the characteristic exponent of K (i.e., $p = \operatorname{char} K$ if this is positive, and $p = 1$ otherwise). Take $f \in K[X]$. Then f is additive if and only if it is of the form*

$$f(X) \;=\; \sum_{i=0}^{m} c_i X^{p^i} \quad \text{with } c_i \in K \;. \tag{2}$$

Assume that $\operatorname{char} K = p > 0$. Then as a mapping on K, X^p is equal to the Frobenius endomorphism φ. Similarly, X^{p^2} is equal to the composition of φ with itself, written as φ^2, and by induction, we can replace 2 by every integer n. On the other hand, the monomial X induces the identity mapping, which we may write as φ^0. Note that addition and composition of additive mappings on $(K,+)$ give again additive mappings (in particular, addition of additive polynomials gives additive polynomials). It remains to interpret the coefficients of additive polynomials as mappings. This is easily done by viewing K as a K-vector space: the mapping $c\cdot$ induced by $c \in K$ is given by multiplication $a \mapsto ca$, and it is an automorphism of $(K,+)$ if $c \neq 0$. So cX^{p^n} as a mapping is the composition of φ^n with $c\cdot$. We will write this composition as $c\varphi^n$. Adding these monomials generates new additive mappings of the form $\sum_{i=0}^{m} c_i\varphi^i$, and addition of such mappings gives again additive mappings of this form. Composition of such additive mappings generates again additive mappings, and the reader may compute that they can again be written in the above form. In this way, we are naturally led to considering the ring $K[\varphi]$ of all polynomials in φ over K, where multiplication is given by composition. From the above we see that this ring is a subring of the endomorphism ring of the additive group of K. The correspondence that we have worked out now reads as

$$\sum_{i=0}^{m} c_i X^{p^i} \quad \longleftrightarrow \quad \sum_{i=0}^{m} c_i \varphi^i \in K[\varphi] \tag{3}$$

which means that both expressions describe the same additive mapping on K. For instance, the additive Artin-Schreier polynomial $X^p - X$ corresponds to $\varphi - 1$. Through the above correspondence, the ring $K[\varphi]$ may be considered as the **ring of additive polynomials over** K. Note that this ring is not commutative; in fact, we have

$$\varphi c = c^p \varphi \quad \text{for all } c \in K \;.$$

This shows that assigning $\varphi \mapsto z$ induces an isomorphism of $K[\varphi]$ onto the skew polynomial ring $K[z;\varphi]$. But we will keep the notation "$K[\varphi]$" since it is simpler.

Let me state some basic properties of the ring $K[\varphi]$. For more information, I recommend the comprehensive book "Free rings and their relations" by P. M. Cohn ([C1], [C2]). Let R be a ring with $1 \neq 0$. Equipped with a function $\deg : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$, the ring

R is called **left euclidean** if for all elements $s, s' \in R$, $s \neq 0$, there exist $q, r \in R$ such that

$$s' = qs + r \quad \text{with} \quad r = 0 \ \text{ or } \ \deg r < \deg s \ ,$$

and it is called **right euclidean** if the same holds with "$s' = sq + r$" in the place of "$s' = qs + r$". (Usually, the function deg is extended to 0 by setting $\deg 0 = -\infty$.) For example, polynomial rings over fields equipped with the usual degree function are both-sided euclidean rings. Further, an integral domain R is called a **left principal ideal domain** if every left ideal in R is principal (and analogously for "right" in the place of "left"). I leave it to the reader to show that every left (or right) euclidean integral domain is a left (or right) principal ideal domain. Finally, an integral domain R is called a **left Ore domain** if

$$Rr \cap Rs \neq \{0\} \quad \text{for all } r, s \in R \setminus \{0\} \ ,$$

and it is called a **right Ore domain** if $rR \cap sR \neq \{0\}$ for all $r, s \in R \setminus \{0\}$. Every left (or right) Ore domain can be embedded into a skew field (cf. [C1], §0.8, Corollary 8.7). The reader may prove that a left (or right) principal ideal domain is a left (or right) Ore domain.

The ring $K[\varphi]$ may be equipped with a degree function which satisfies $\deg 0 = -\infty$ and $\deg \sum_{i=0}^{m} c_i \varphi^i = m$ if $c_m \neq 0$. This degree function is a homomorphism of the multiplicative monoid of $K[\varphi] \setminus \{0\}$ onto $\mathbb{N} \cup \{0\}$ since it satisfies $\deg rs = \deg r + \deg s$. In particular, this shows that $K[\varphi]$ is an integral domain. The following theorem is due to O. Ore [O2]; I will give a proof in Section 4.

Theorem 2 *The ring $K[\varphi]$ is a left euclidean integral domain and thus also a left principal ideal domain and a left Ore domain. It is right euclidean if and only if K is perfect; if K is not perfect, then $K[\varphi]$ is not even right Ore.*

Example 1 Let $\mathbb{F}_p$ denote the field with p elements. The ring $\mathbb{F}_p[\varphi]$ is a both-sided euclidean integral domain, and every field K of characteristic p is a left $\mathbb{F}_p[\varphi]$-module and a left $K[\varphi]$-module, where the action of φ on K is just the application of the Frobenius endomorphism. K is perfect if and only if every element of K is divisible by the ring element φ. But this does not imply that K is a divisible $\mathbb{F}_p[\varphi]$- or $K[\varphi]$-module. For instance, if K admits non-trivial Artin-Schreier extensions, that is, if $K \neq \wp(K) = (\varphi - 1)K$, then there are elements in K which are not divisible by $\varphi - 1$. On the other hand, K is a divisible $\mathbb{F}_p[\varphi]$- and $K[\varphi]$-module if K is algebraically closed.

Observe that K is not torsion free as an $\mathbb{F}_p[\varphi]$- or $K[\varphi]$-module. Indeed, K contains $\mathbb{F}_p$ which satisfies

$$(\varphi - 1)\mathbb{F}_p = \{0\} \ .$$

$\diamondsuit$

Example 2 The power series field $K := \mathbb{F}_p((t)) = \{\sum_{i=N}^{\infty} c_i t^i \mid N \in \mathbb{Z}\,,\, c_i \in K\}$ (also called "field of formal Laurent series over $\mathbb{F}_p$") is not perfect, since t does not admit a p-th root in K. Hence, the ring $K[\varphi]$ is not right Ore. K is a left $K[\varphi]$-module. $\diamondsuit$

In Section 4, Remark 24, I will collect a few properties of the rings $K[\varphi]$ that follow from Theorem 2, and describe what happens if K is not perfect. We will see that in that case the structure of $K[\varphi]$-modules becomes complicated. It seems that the "bad" properties of $K[\varphi]$, for K non-perfect, are symptomatic for the problems algebraists and model theorists have with non-perfect valued fields in positive characteristic. Let me discuss the most prominent of such non-perfect valued fields.

The field $\mathbb{F}_p((t))$ carries a canonical valuation v_t, called the t-adic valuation. It is given by $v_t \sum_{i=N}^{\infty} c_i t^i = N$ if $c_N \neq 0$ and $v_t 0 = \infty$. $(\mathbb{F}_p((t)), v_t)$ is a complete discretely valued field, with value group $v_t \mathbb{F}_p((t)) = \mathbb{Z}$ (that is what "discretely valued" means) and residue field $\mathbb{F}_p((t))v_t = \mathbb{F}_p$. At the first glance, such fields may appear to be the best known objects in valuation theory. Nevertheless, the following prominent questions about the elementary theory $\mathrm{Th}(\mathbb{F}_p((t)), v_t)$ are still unanswered:

Open Problem 1 Is the elementary theory of the valued field $\mathbb{F}_p((t))$ model complete? Does it admit quantifier elimination in some natural language? Is it decidable? If yes, what would be a complete recursive axiomatization?

The corresponding problem for the p-adics was solved in the mid 1960s independently by Ax and Kochen [A–K] and by Ershov [E]. Since then, the above problem has been well known to model-theoretic algebraists, but resisted all their attacks.

Encouraged by the similarities between $\mathbb{F}_p((t))$ and the field $\mathbb{Q}_p$ of p-adic numbers, one might try to give a complete axiomatization for $\mathrm{Th}(\mathbb{F}_p((t)), v_t)$ by adapting the well known axioms for $\mathrm{Th}(\mathbb{Q}_p, v_p)$. They express that $(\mathbb{Q}_p, v_p)$ has the following elementary properties:

- It is a henselian valued field of characteristic 0. A valued field (K, v) is called henselian if it satisfies Hensel's Lemma: *If f is a polynomial with coefficients in the valuation ring $\mathcal{O}$ of v and if $b \in \mathcal{O}$ such that $vf(b) > 0$ while $vf'(b) = 0$, then there is some $a \in \mathcal{O}$ such that $f(a) = 0$ and $v(a - b) > 0$.* This holds if and only if the extension of v to the algebraic closure of K is unique.
- Its value group a $\mathbb{Z}$-group, i.e., an ordered abelian group elementarily equivalent to $\mathbb{Z}$.
- Its residue field is $\mathbb{F}_p$.
- $v_p p$ is equal to 1 (= the smallest positive element in the value group).

The last condition is not relevant for $\mathbb{F}_p((t))$ since there, $p \cdot 1 = 0$. Nevertheless, we may add a constant name t to $\mathcal{L}$ so that one can express by an elementary sentence that $v_t t = 1$.

A naive adaptation would just replace "characteristic 0" by "characteristic p" and p by t. But there is an elementary property of valued fields that is satisfied by all valued

fields of residue characteristic 0 and all formally p-adic fields, but not by all valued fields in general. It is the property of being defectless. A valued field (K,v) is called **defectless** if for every finite extension $L|K$, equality holds in the **fundamental inequality**

$$n \ \geq \ \sum_{i=1}^{\mathrm{g}} \mathrm{e}_i \mathrm{f}_i \ , \tag{4}$$

where $n=[L:K]$ is the degree of the extension, $v_1,\ldots,v_{\mathrm{g}}$ are the distinct extensions of v from K to L, $\mathrm{e}_i=(v_iL:vK)$ are the respective ramification indices, and $\mathrm{f}_i=[Lv_i:Kv]$ are the respective inertia degrees. (Note that $\mathrm{g}=1$ if (K,v) is henselian.) There is a simple example, due to F. K. Schmidt, which shows that there is a henselian discretely valued field of positive characteristic which is not defectless (cf. [Ri], Exemple 1, p. 244). This field has a finite purely inseparable extension with non-trivial defect. But defect does not only appear in purely inseparable extensions: there is an example, due to A. Ostrowski, of a complete valued field admitting a finite separable extension with non-trivial defect (cf. [Ri], Exemple 2, p. 246). These and several other examples of extensions with non-trivial defect of various types can also be found in [Ku12] (see also [Ku8]).

However, each power series field with its canonical valuation is henselian and defectless (cf. [Ku12]). In particular, $(\mathbb{F}_p((t)),v_t)$ is defectless. For a less naive adaptation of the axiom system of $\mathbb{Q}_p$, we will thus add "defectless". We obtain the following axiom system in the language $\mathcal{L}(t)=\mathcal{L}\cup\{t\}$:

$$\left.\begin{array}{l}(K,v) \text{ is a henselian defectless valued field}\\ K \text{ is of characteristic } p\\ vK \text{ is a } \mathbb{Z}\text{-group}\\ Kv=\mathbb{F}_p\\ vt \text{ is the smallest positive element in } vK\ .\end{array}\right\} \tag{5}$$

Let us note that also $(\mathbb{F}_p(t),v_t)^h$, the henselization of $(\mathbb{F}_p(t),v_t)$, satisfies these axioms. The **henselization** of a valued field (K,v) is a henselian algebraic extension which is minimal in the sense that it admits a (unique!) embedding over K in every henselian extension of (K,v). Henselizations exist for all valued fields, and they are separable extensions (cf. [Ri], Théorème 2, p. 176). It is well known that $(\mathbb{F}_p(t),v_t)^h$ is a defectless field, being the henselization of a global field (cf. [Ku9]). It is also well known that $(\mathbb{F}_p(t),v_t)^h$ is existentially closed in $(\mathbb{F}_p((t)),v_t)$ (see below for the definition of this notion); this fact follows from work of Greenberg [Gre] and also from Theorem 2 of [Er1] (see also [Ku7] for some related information). But it is not known whether $(\mathbb{F}_p((t)),v_t)$ is an elementary extension of $(\mathbb{F}_p(t),v_t)^h$.

It did not seem unlikely that axiom system (5) could be complete, until I proved in [Ku1] (cf. [Ku4]):

Theorem 3 *The axiom system (5) is not complete.*

I will give an idea of the proof of this theorem in Section 2.3 below. It was inspired by an observation of Lou van den Dries. He had worked with a modified axiom system (with larger residue fields) and had found an elementary sentence which he was not able to deduce from that axiom system (as it turned out, that wasn't van den Dries' fault). This sentence was formulated using only addition, multiplication with the element t and application of the Frobenius, but no general multiplication. This led van den Dries to the question whether one could at least determine the model theory of $\mathbb{F}_p((t))$ as a module which admits multiplication with t and application of the Frobenius, forgetting about general multiplication. But this means that we view $\mathbb{F}_p((t))$ as a left $K[\varphi]$-module, where the field K contains t and should be contained in $\mathbb{F}_p((t))$. But then, K is not perfect, and therefore the structure of $K[\varphi]$-modules may be quite complicated.

There is a common feeling that additive polynomials play a crucial role in the theory of valued fields of positive characteristic. So indeed, van den Dries' question may be the key to the model theory of $\mathbb{F}_p((t))$ (but it could be as hard to solve as the original problem). In this paper, I will give some reasons for this common feeling, but also confront it with our present problem of understanding the notion of extremality.

2.1 Reason #1: Kaplansky's hypothesis A

For a valued field (K, v), we denote by vK its value group and by Kv its residue field. An extension $(K, v) \subset (L, v)$ of valued fields is called **immediate** if the induced embeddings of vK in vL and of Kv in Lv are onto. Henselizations are immediate extensions (cf. [Ri], Corollaire 1, p. 184). Wolfgang Krull [Kr] (see also [Gra]) proved that every valued field admits a maximal immediate extension. A natural and in fact very important question is whether this is unique up to (valuation preserving) isomorphism. This plays a role when one wishes to embed valued fields in power series fields. In his celebrated paper [Ka1], Irving Kaplansky gave a criterion, called "hypothesis A", which guarantees uniqueness. (We will present it later.) Kaplansky then showed that a valued field (K, v) of positive characteristic having a cross-section and satisfying hypothesis A can be embedded in the power series field $Kv((vK))$ over its residue field Kv with exponents in its value group vK. Kaplansky also gives examples which show that this may fail if hypothesis A is not satisfied. In this case, there are **maximal fields** (= valued fields not admitting any proper immediate extensions) which do not have the form of a power series field (not even if one allows factor systems).

If we are considering an elementary class of valued fields satisfying hypothesis A (which can be expressed by a recursive scheme of elementary sentences in the language of valued rings), then the uniqueness of maximal immediate extensions can be fruitfully used in the proof of model theoretic properties. Let us give the example of algebraically maximal Kaplansky fields. A valued field is called **algebraically maximal** if it does not admit any proper immediate algebraic extension. It is called a **Kaplansky field** if it satisfies hypothesis A. The following theorem is due to Ershov [Er1] and, independently, Ziegler

[Zi].

Theorem 4 *The elementary theory of an algebraically maximal Kaplansky field is completely determined by the elementary theory of its value group and the elementary theory of its residue field.*

In other words, algebraically maximal Kaplansky fields satisfy the following **Ax–Kochen–Ershov principle**:

$$vK \equiv vL \wedge Kv \equiv Lv \implies (K,v) \equiv (L,v) \tag{6}$$

where the first elementary equivalence is in the language of ordered groups, the second in the language of rings and the third in the language of valued rings. In the case of $(K,v) \subseteq (L,v)$ there is also a version of the Ax–Kochen–Ershov principle with "$\equiv$" replaced by "$\prec$" (elementary extension). In the same situation, there is also the more basic version

$$vK \prec_\exists vL \wedge Kv \prec_\exists Lv \implies (K,v) \prec_\exists (L,v) \tag{7}$$

where "$\prec_\exists$" means "**existentially closed in**", that is, every existential elementary sentence which holds in the upper structure also holds in the lower structure. In fact, it has turned out that proving this version is the essential step in proving Ax–Kochen–Ershov principles and other model theoretic results about valued fields; the further results then often follow by general model theoretic arguments (the reader should think of Robinson's Test).

Hypothesis A implicitly talks about additive polynomials. Following Kaplansky [Ka2], we will call a polynomial $f \in K[X]$ a **p-polynomial** if it is of the form

$$f(X) = \mathcal{A}(X) + c\,, \tag{8}$$

where $\mathcal{A} \in K[X]$ is an additive polynomial, and c is a constant in K. A field K of characteristic $p > 0$ will be called **p-closed** if every p-polynomial in $K[X]$ has a root in K. That is,

K is p-closed if and only if it is a divisible $K[\varphi]$-module.

In particular, every p-closed field is perfect.

Now hypothesis A for a valued field (K,v) with $\operatorname{char} Kv = p > 0$ reads as follows:

(A1) the value group vK is p-divisible, and

(A2) the residue field Kv is p-closed.

For valued fields (K,v) with $\operatorname{char} Kv = 0$, hypothesis A is empty. The condition of a field to be p-closed seemed obscure at the time of Kaplansky's paper. But we have learned to understand this condition better. The following theorem was first proved by Whaples in [Wh2], using the cohomology theory of additive polynomials. A more elementary proof was later given in [Del]. Then Kaplansky gave a short and elegant proof in his "Afterthought: Maximal Fields with Valuation" ([Ka2]). We will reproduce this proof in Section 9.

Theorem 5 *A field K of characteristic $p > 0$ is p-closed if and only if it does not admit any finite extensions of degree divisible by p.*

This theorem lets us understand hypothesis A much better. Based on this insight, Kaplansky's result about uniqueness of maximal immediate extensions is reproved in [Ku–Pa–Ro]. There, it is deduced from the Schur–Zassenhaus Theorem about conjugacy of complements in profinite groups, via Galois correspondence.

As we are shifting our focus to additive polynomials, the original condition "p-closed" regains its independent interest. In Section 9 we will use Theorem 5 to prove:

Theorem 6 *A henselian valued field of characteristic $p > 0$ is p-closed if and only if it is an algebraically maximal Kaplansky field.*

For a generalization of the notion "p-closed" and of this theorem to fields of characteristic 0 see [V], in particular Corollary 5.

By Theorem 5 we can split condition (A2) into two distinct conditions:

(A2.1) the residue field Kv is perfect, and

(A2.2) the residue field Kv does not admit any finite separable extension of degree divisible by p.

While (A2.1) is a perfectly natural condition about fields, (A2.2) is somewhat unusual. This is the reason for the fact that Kaplansky fields are not often found in applications. Certainly also the other conditions restrict the possible applications (for example, $\mathbb{F}_p((t))$ doesn't satisfy (A1)). But for instance, every perfect valued field of characteristic $p > 0$ satisfies conditions (A1) and (A2.1) (but not necessarily (A2.2)). So we would obtain a more natural condition if we could drop condition (A2.2). To obtain good model theoretic properties for fields satisfying (A1) and (A2.1), one has to require again that they are algebraically maximal. Such fields form a part of an important larger class of valued fields, the tame fields. A **tame field** is a henselian field whose algebraic closure is equal to the ramification field K^r of the normal extension $K^{\text{sep}}|K$, where K^{sep} denotes the separable-algebraic closure of K. The **ramification field** of a normal separable-algebraic extension of valued fields is the fixed field in that extension of a certain subgroup of the Galois group, the **ramification group**. We don't need the definition of this group here; we only need the basic properties of the field K^r which I will put together in Theorem 38 below. By part e) of this theorem, every tame field is defectless, and it follows directly from the definition that every tame field is perfect. In [Ku1] (cf. also [Ku11]) I proved:

Theorem 7 *The elementary theory of a tame field is completely determined by the elementary theory of its value group and the elementary theory of its residue field.*

All tame fields satisfy conditions (A1) and (A2.1), but not necessarily (A2.2). That means that we have lost the uniqueness of maximal immediate extensions. But the above result shows that uniqueness is not necessary for an elementary class of valued fields to have good model theoretic properties. However, we have to work much harder. This work is again directly related to additive polynomials, and we will describe this connection now.

2.2 Reason #2: the defect and purely wild extensions

Let us assume that (K, v) is henselian. Then for every finite extension L of K, we have $g = 1$ in the fundamental inequality (4). Then the Lemma of Ostrowski (cf. [Ri], Théorème 2, p. 236) tells us that we have an equality

$$[L : K] \;=\; (vL : vK) \cdot [Lv : Kv] \cdot p^{\delta} \;, \tag{9}$$

where p is the characteristic exponent of the residue field Kv, and δ is a non-negative integer. The factor p^{δ} is called the **defect** of the extension $(L|K, v)$; it is **trivial** if $p^{\delta} = 1$. Consequently, every valued field with residue field of characteristic 0 is defectless.

It follows from Theorem 38 that a valued field is tame if it is henselian and for every finite extension $L|K$,

- the characteristic of Kv does not divide $(vL : vK)$,
- the extension $Lv|Kv$ is separable, and
- the extension $(L|K, v)$ is defectless.

The ramification field K^r is the unique maximal tame extension of every henselian field (K, v).

As I have explained in [Ku3], the presence of non-trivial defect is one of the main obstacles in proving an Ax–Kochen–Ershov principle like (7). Let me quickly sketch this again. Assume that (L, v) is an extension of a henselian field (K, v) such that $vK \prec_\exists vL$ and $Kv \prec_\exists Lv$. Then we take (K^*, v^*) to be an $|L|^+$-saturated elementary extension of (K, v). It follows that v^*K^* is a $|vL|^+$-saturated extension of vK; hence $vK \prec_\exists vL$ yields that vL can be embedded over vK in v^*K^*. It also follows that K^*v^* is an $|Lv|^+$-saturated extension of vL; hence $Kv \prec_\exists Lv$ yields that Lv can be embedded over Kv in K^*v^*. Now we have to lift these embeddings to an embedding of (L, v) in (K^*, v^*) over K. Once this is achieved, we are done, because every existential elementary sentence which holds in (L, v) carries over to its image in (K^*, v^*), from there up to (K^*, v^*), and from there down to the elementary substructure (K, v).

By a general model theoretic argument, the situation can be reduced to the case where L is finitely generated over K. That is, $(L|K, v)$ is a valued function field (by "function field", we will always mean "algebraic function field"). Hence, we need the structure theory of valued function fields to solve our embedding problem (as it is the case for the problem of local uniformization). Let us assume that we can reduce to the case where the transcendence degree of $L|K$ is 1. This can be done for tame fields, but for the model theory of $\mathbb{F}_p((t))$, this is another serious problem, again connected with additive polynomials (see Section 2.3). Assume further that we have lifted the embeddings of vL and Lv to an embedding of some subfield L_0 of L. Then $L|L_0$ is a finite immediate extension, and in general, it will be proper (i.e., $L \neq L_0$). Taking henselizations, we obtain that also $L^h|L_0^h$ is a finite immediate extension. Since we assumed that (K, v) is henselian (which is true for every algebraically maximal and every tame field), its

elementary extension (K^*, v^*) is also henselian. Therefore, the embedding of L_0 extends to an embedding of L_0^h in K^* (this is the universal property of the henselization). But if $L^h \neq L_0^h$, we do not know how to lift the extension further (which we would need to get all of L embedded), unless we have uniqueness of maximal immediate extensions. Since $L^h|L_0^h$ is immediate, we have $(vL^h : vL_0^h) = 1$ and $[L^h v : L_0^h v] = 1$; hence if $L^h \neq L_0^h$, then by (9), the extension has non-trivial defect, equal to its degree.

We see that indeed, the presence of non-trivial defect constitutes a serious obstacle for our embedding problem. So we have to avoid the defect. In certain cases, it will not even appear. All tame fields are defectless fields (and so are all other valued fields for which we know good model theoretic results). This does not mean that every valued function field over a tame field is defectless. But for a certain type of valued function fields, this is true. Let $(L|K, v)$ be an extension of valued fields of finite transcendence degree. Then the following inequality holds (cf. [B], Chapter VI, §10.3, Theorem 1):

$$\operatorname{trdeg} L|K \;\geq\; \dim_{\mathbb{Q}}(\mathbb{Q} \otimes (vL/vK)) \;+\; \operatorname{trdeg} Lv|Kv \;. \tag{10}$$

If equality holds then we will say that $(L|K, v)$ **is without transcendence defect**. For such function fields, we have ([Ku1], [Ku9]):

Theorem 8 (Generalized Stability Theorem) *Let $(L|K, v)$ be a valued function field without transcendence defect. If (K, v) is a defectless field, then also (L, v) is a defectless field.*

Using this theorem, one can prove (cf. [Ku9]):

Theorem 9 *Let (K, v) be a henselian defectless field. Then the Ax–Kochen–Ershov principle (7) holds for every extension (L, v) of (K, v) without transcendence defect.*

I proved Theorem 8 in [Ku1]. How does this proof work? How can we see whether a given valued field is defectless? First of all, a valued field is defectless if and only if its henselization is (see [Ku9]; a partial proof is also given in [En]). So we can assume that L is the henselization of a valued function field. Second, if (k, v) is any henselian field, then every finite extension of k inside the ramification field k^r has trivial defect, and if $k_1|k$ is any finite extension, then $k_1|k$ and $k^r.k_1|k^r$ have the same defect (cf. Theorem 38). So in our situation, we have to show that every finite extension of L^r has trivial defect. The advantage of working over L^r is that general ramification theory tells us that $L^{\rm sep}|L^r$ is a p-extension. A normal and separable field extension is called a **p-extension** if its Galois group is a pro-p-group. It follows from the general theory of p-groups (cf. [H], Chapter III, §7, Satz 7.2 and the following remark) via Galois correspondence that every finite separable-algebraic extension of L^r is a tower of Galois extensions of degree p. Hence we just have to show by induction that each of them has trivial defect. (The complementary case of purely inseparable extensions is much easier and can be disposed of more directly.) Now every Galois extension $k'|k$ of degree p of fields of characteristic p is an Artin-Schreier

extension; this well known fact is proved by an application of Hilbert's Theorem 90. We include a proof in Section 7 (Theorem 35), as a special case of a generalization which we will discuss below.

Let ϑ be a root of $X^p - X - a$. Then $k' = k(\vartheta) = k(\vartheta - c)$ for every $c \in k$. As $X^p - X$ is an additive polynomial, we have $(\vartheta - c)^p - (\vartheta - c) = a - c^p + c$, that is, $\vartheta - c$ is a root of the p-polynomial $X^p - X - (a - c^p + c)$. So we may change a by subtracting elements in k of the form $c^p - c$, without changing the extension generated by the polynomial. The idea in our above situation is now to find by this method a suitable normal form for the element a from which we can read off that the extension has trivial defect. The idea of deducing suitable normal forms for Artin-Schreier extensions (and for Kummer extensions in the case of fields of characteristic 0) can already be found in the work of Hasse, Whaples, Epp ([Ep], see also [Ku5]), Matignon and Abhyankar.

Let us quickly discuss two examples. We wish to show that a given Artin-Schreier extension $L'|L^r$ has trivial defect. Before we go on, we note that by valuation theoretical arguments, the proof of Theorem 8 can be reduced to the case where K and hence also its residue field Kv is algebraically closed. Assume that the transcendence degree of $L|K$ is 1. Then by (10) with equality, we can have

- $\dim_{\mathbb{Q}}(\mathbb{Q} \otimes (vL/vK)) = 1$ and $\operatorname{trdeg} Lv|Kv = 0$, or
- $\dim_{\mathbb{Q}}(\mathbb{Q} \otimes (vL/vK)) = 0$ and $\operatorname{trdeg} Lv|Kv = 1$.

In the first case, there is an element $x \in L$ such that vx is rationally independent over vK. Under certain additional conditions, we can then take a to be a polynomial in x with coefficients in K. Since the values of the monomials in this polynomial $a = a(x)$ lie in distinct cosets modulo vK, their values are distinct. By the ultrametric triangle law, this implies that the value of such a monomial is equal to the least value of its monomials. Now we can use the above method to get rid of p-th powers of x in $a(x)$ (we can replace a monomial cx^{kp} by $c^{1/p}x^k$. Therefore, we can assume that all monomials appearing in the polynomial $a(x)$ are of the form $c_i x^i$ with i not divisible by p. Then the value $va(x)$ is not divisible by p in vL^r. This value cannot be positive since otherwise, the extension would be trivial by Hensel's Lemma. With the value being negative, the reader may show that if ϑ is a root of $X^p - X - a(x)$, then

$$v\vartheta \;=\; \frac{va(x)}{p}\;.$$

This implies that $(vL' : vL^r) = p = [L' : L^r]$, so the extension has trivial defect.

In the second case, we will have an element $x \in L$ of value 0 whose residue xv is transcendental over Kv. Now we will have to deal with finite sums of the form $c_i d_i$ where $d_i \in L$ are representatives of elements in the residue field. We play the same game as before, trying to come up with a residue that has no p-th root, from which it would follow in a similar way as above that $[L'v : L^r v] = p = [L' : L^r]$, showing that the extension has trivial defect. The problem here is that when we replace some monomial $c_i d_i$ by its p-th

root $c_i^{1/p} d_i^{1/p}$, then even if the residue $d_i^{1/p} v$ does not have a p-th root in Lv, the element $d_i^{1/p}$ might sum up with some other d_j to an element whose residue has again a p-th root in Lv. We somehow have to see that this process cannot go on infinitely. A good idea would be to take the d_i such that their residues form a basis of $Lv|Kv$. But then we would need that also the residue of $d_i^{1/p}$ is in this basis. It is easily seen that a basis being closed under taking p-th roots (as long as we stay in Lv) is the same as a basis being closed under taking p-th powers (in other words, being closed under the Frobenius). Such a basis will be called a **Frobenius-closed basis**. See Lemma 25 which gives the exact formulation of the property of a Frobenius-closed basis that we need in [Ku9].

The residue field of $K(x)$ is just $Kv(xv)$. Further, L being a function field of transcendence degree 1, $L|K(x)$ is a finite extension. It follows from the fundamental inequality that also $Lv|K(x)v$ is a finite extension. This shows that $Lv|Kv$ is a function field of transcendence degree 1. So in order to prove our theorem in the second case, our task is to find a Frobenius-closed basis for every function field of transcendence degree 1 over an algebraically closed field of positive characteristic. In [Ku1], I proved a more general result:

Theorem 10 *Let F be an algebraic function field of transcendence degree 1 over a perfect field K of characteristic $p > 0$. If K is relatively algebraically closed in F, then there exists a Frobenius-closed basis for $F|K$.*

The proof and some further background are given in Section 5. There, we will also deduce the following result from Theorem 10, showing the connection between Frobenius-closed bases and additive polynomials:

Theorem 11 *If F is an algebraic function field of transcendence degree 1 over a perfect field K of characteristic $p > 0$ and if K is relatively algebraically closed in F, then F/K is a free $K[\varphi]$-module.*

The second important theorem that I use in the proof of Theorem 7 is needed when the valued function field $(L|K, v)$ has non-trivial transcendence defect, i.e., equality does not hold in (10). In reducing to transcendence degree 1 by induction, one reaches the case where (L, v) is an immediate extension of transcendence degree 1 of the tame field (K, v). The defect is then avoided by means of the following theorem.

Theorem 12 (Henselian Rationality)
Let (K, v) be a tame field and $(L|K, v)$ an immediate function field of transcendence degree 1. Then the henselization $(L, v)^h$ of (L, v) is **henselian rational***, i.e.,*

$$\text{there is } x \in L \text{ such that } \; L^h = K(x)^h \; . \tag{11}$$

For valued fields of residue characteristic 0, the assertion is a direct consequence of the fact that every such field is defectless (in fact, every $x \in L \setminus K$ will then do the job). In contrast to this, the case of positive residue characteristic requires a much deeper structure theory of immediate algebraic extensions of henselian fields, in order to find suitable elements x. I proved this theorem in [Ku1] (cf. also [Ku10]).

The proof works as follows. Suppose we have chosen the wrong x. Then the extension $L^h|K(x)^h$ is proper and immediate. So by (9) its defect is equal to its degree and thus non-trivial. If $L^h|K(x)^h$ were an Artin-Schreier extension, we could employ the same methods as described above to find a normal form that allows us to find a better x (i.e., one for which the degree $[L^h : K(x)^h]$ is smaller). But in general, even if $L^h|K(x)^h$ is separable, it will not necessarily be a tower of Artin-Schreier extensions. Note that because its degree is a prime, an Artin-Schreier extension does not admit any proper subextensions; such an extension is called **minimal**. This leads us to the following question: what is the structure of minimal subextensions of such extensions $L^h|K(x)^h$?

Since $L^h|K(x)^h$ is immediate, but every finite subextension of $K(x)^r|K(x)^h$ (where $K(x)^r := (K(x)^h)^r$) is defectless by part e) of Theorem 38, it follows that $L^h|K(x)^h$ is linearly disjoint from $K(x)^r|K(x)^h$. Take any henselian field (k, v). Then an algebraic extension k_1 is called **purely wild** if $k_1|k$ is linearly disjoint from $k^r|k$. Hence, our extension $L^h|K(x)^h$ is purely wild. Our question is now answered by the following theorem, which again shows the importance of p-polynomials and hence also of additive polynomials. This theorem is due to Florian Pop ([Pop]).

Theorem 13 *Let (k, v) be a henselian field of characteristic $p > 0$ and $(k_1|k, v)$ a minimal purely wild extension. Then there exist an additive polynomial $\mathcal{A}(X) \in \mathcal{O}_k[X]$ and an element $\vartheta \in k_1$ such that $k_1 = k(\vartheta)$ and the p-polynomial $\mathcal{A}(X) - \mathcal{A}(\vartheta)$ is the minimal polynomial of ϑ over k.*

It can be shown using Hensel's Lemma that if $k_1 \neq k$, then $\mathcal{A}(\vartheta) \notin \mathcal{O}_k$.

Using the additivity of the polynomial $\mathcal{A}$ like I used the additivity of the Artin-Schreier polynomial $X^p - X$ before, it is indeed possible to deduce a normal form that allows to find a better x. Therefore, Theorem 13 is an important ingredient in the proof of Theorem 12. Three sections of this paper are devoted to the previously unpublished proof of Theorem 13. For the convenience of the reader, G-modules and twisted homomorphisms are introduced in Section 6. In Section 7, a Galois theoretical result of independent interest is proved. It is a generalization of the theorem that I have already used above and that states that every Galois extension of degree p in characteristic p is an Artin-Schreier extension. Then I apply it in Section 8 to the situation of purely wild extensions and derive Theorem 13.

Theorem 13 gains even more importance in conjunction with a result of Matthias Pank (see [Ku–Pa–Ro]):

Theorem 14 *Let (K, v) be a henselian field. Then K^r admits a field complement W in the algebraic closure $\tilde{K}$, that is, $W.K^r = \tilde{K}$ and $W \cap K^r = K$. Every such complement W is a maximal purely wild extension of K. The quotient group vW/vK is a p-group (where p is the characteristic exponent of Kv), and the extension $Wv|Kv$ is purely inseparable.*

Note that (K, v) is a tame field if and only if $W = K$.

2.3 Reason #3: extremality and elementary properties of additive polynomials

If f is a polynomial in n variables with coefficients in K, then we will say that (K, v) is **extremal with respect to** f if the set

$$\{vf(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in K\} \subseteq vK \cup \{\infty\} \tag{12}$$

has a maximum. This means that

$$\exists Y_1, \ldots, Y_n \forall X_1, \ldots, X_n vf(X_1, \ldots, X_n) \leq vf(Y_1, \ldots, Y_n)$$

holds in (K, v). It follows that being extremal with respect to f is an elementary property in the language of valued fields with parameters from K. Note that the maximum is ∞ if and only if f admits a K-rational zero. A valued field (K, v) is called **extremal** if for all $n \in \mathbb{N}$, it is extremal with respect to every polynomial f in n variables with coefficients in K. This notion is due to Ershov. The property of being extremal can be expressed by a countable scheme of elementary sentences (quantifying over the coefficients of all possible polynomials of degree at most n in at most n variables). Hence, it is elementary in the language of valued fields.

The following result was first stated by Delon in [Del], but the proof contained gaps. The gaps were later filled by Ershov in [Er2]. I give an alternative proof in [Ku8].

Theorem 15 *A valued field is algebraically maximal if and only if it is extremal with respect to every polynomial in one variable.*

The following related results, also proved in [Ku8], illustrate again the importance of additive and p-polynomials. First, using Theorem 13, we can push the result stated in Theorem 15 even further:

Theorem 16 *A henselian valued field of characteristic $p > 0$ is algebraically maximal if and only if it is extremal with respect to every p-polynomial in one variable.*

A polynomial $\mathcal{A} \in K[X_1, \ldots, X_n]$ in n variables is called **additive** if for all elements $a_1, \ldots, a_n, b_1, \ldots, b_n$ in any extension field of K,

$$\mathcal{A}(a_1 + b_1, \ldots, a_n + b_n) \;=\; \mathcal{A}(a_1, \ldots, a_n) \;+\; \mathcal{A}(b_1, \ldots, b_n)\;.$$

In fact, if $\mathcal{A}$ is additive then

$$\mathcal{A}(X_1, \ldots, X_n) \;=\; \sum_{i=1}^{n} \mathcal{A}_i(X_i)$$

where

$$\mathcal{A}_i(X_i) \;:=\; \mathcal{A}(0, \ldots, 0, X_i, 0, \ldots, 0)$$

are additive polynomials in one variable. As before, a polynomial $f \in K[X_1, \ldots, X_n]$ in n variables is called **p-polynomial** if it is of the form $\mathcal{A} + c$ where $\mathcal{A} \in K[X_1, \ldots, X_n]$ is additive, and $c \in K$. From the above we see that also every p-polynomial is a sum of p-polynomials in one variable.

A valued field is called **inseparably defectless** if all purely inseparable extensions have trivial defect. The following is proved in [Ku8]:

Theorem 17 *A valued field (K, v) of characteristic $p > 0$ is inseparably defectless if and only if it is extremal with respect to every p-polynomial of the form*

$$b - \sum_{i=1}^{n} b_i X_i^p \;, \qquad n \in \mathbb{N},\; b, b_1, \ldots, b_n \in K \;. \tag{13}$$

Observe that again, all of these notions can be axiomatized by recursive elementary axiom schemes.

I will now sketch the basic idea of the proof of Theorem 3. Note that the image of a polynomial f on a valued field K has the *optimal approximation property* in the sense of [Ku4] and [Dr–Ku] if and only if K is extremal with respect to $f - c$ for every $c \in K$. Consequently,

the images of all additive polynomials over (K, v) have the optimal approximation property if and only if K is extremal with respect to all p-polynomials over K.

This holds in one variable as well as in several variables.

In [Ku4], I considered the following additive polynomial over $\mathbb{F}_p((t))$:

$$X_0^p - X_0 \;+\; tX_1^p \;+\; \ldots \;+ t^{p-1} X_{p-1}^p \;. \tag{14}$$

I showed that the image of this polynomial has the optimal approximation property in $\mathbb{F}_p((t))$. Then I constructed an extension (L, v) of $\mathbb{F}_p((t))$ of transcendence degree 1 which is henselian, defectless, has value group a $\mathbb{Z}$-group, with vt the smallest positive element, and residue field $\mathbb{F}_p$, but the image of the above polynomial does not have the optimal approximation property in (L, v). This shows that $\mathbb{F}_p((t))$ with its t-adic valuation is not an elementary substructure of (L, v). This yields Theorem 3.

Further, I proved in [Ku4] that in all maximal fields, the images of all additive polynomials which satisfy a certain elementary condition have the optimal approximation property. Maximal fields are interesting objects in the model theory of valued fields because

all maximal immediate extensions of a valued field are maximal. So if we are considering an elementary class of valued fields closed under maximal immediate extensions (so far, this is the case for all classes of valued fields without additional structure that play a role in model theory), and if the Ax–Kochen–Ershov principle (6) holds for this class, then every field in the class should be elementarily equivalent to all of its maximal immediate extensions. Therefore, the following question is very important:

Open Problem 2 Is every maximal field of characteristic $p > 0$ extremal with respect to every p-polynomial in several variables? Is every maximal field extremal?

Since every maximal field is algebraically maximal, Theorem 15 shows that it is at least extremal with respect to every polynomial in one variable. To answer the first question to the affirmative, one would have to eliminate the condition in the result mentioned above.

In [Ku4], I also construct an immediate function field (F, v) of transcendence degree 1 over (L, v) such that (L, v) is not existentially closed in (F, v). Any maximal immediate extension (M, v) of (F, v) is also a maximal immediate extension of (L, v). Since (L, v) is not existentially closed in (F, v), it is not existentially closed in (M, v). So it is not an elementary substructure of (M, v), and it cannot lie in an elementary class which has the good properties discussed above.

The function field F is generated over L by two elements x_0, x_1 which satisfy an equation

$$x \;=\; x_0^p - x_0 + t x_1^p$$

where x is an element in L which is transcendental over $\mathbb{F}_p((t))$. So the existential sentence

$$\exists X_0 \exists X_1 :\; x \;=\; X_0^p - X_0 + t X_1^p$$

holds in F. On the other hand, L is constructed in such a way that this sentence does not hold in L. This proves that L is not existentially closed in F and, a fortiori, (L, v) is not existentially closed in (F, v).

The function field $F|L$ shows the following interesting symmetry between a generating Artin-Schreier extension and a generating purely inseparable extension of degree p. On the one hand, we have the Artin-Schreier extension

$$L(x_0, x_1)|L(x_1)$$

given by

$$x_0^p - x_0 \;=\; x - t x_1^p \;. \tag{15}$$

On the other hand we have the purely inseparable extension

$$L(x_0, x_1)|L(x_0)$$

given by

$$x_1^p \;=\; \frac{1}{t}(-x_0^p + x_0 + x) \;.$$

From equation (15) it is immediately clear that the function field $L(x_0, x_1)$ becomes rational after a constant field extension by $t^{1/p}$; namely

$$F(t^{1/p}) \;=\; L(t^{1/p})(x_0 + t^{1/p}x_1) \;.$$

This shows that the base field L, not being existentially closed in the function field F, becomes existentially closed in the function field after a finite purely inseparable constant extension, although this extension is linearly disjoint from $F|L$.

In our above example there also exists a separable constant field extension $L'|L$ of degree p such that $(F.L')^h$ is henselian rational. To show this, we take a constant $d \in L$ and an element a in the algebraic closure of L satisfying

$$t \;=\; a^p - da \;,$$

and we put $L' = L(a)$. If we choose d with a sufficiently high value, then we will have that $vdax_1^p > 0$. From this we deduce by Hensel's Lemma that there is an element $b \in L'(x_1)^h$ such that $b^p - b = -dax_1^p$. If we put $z = x_0 + ax_1 + b \in L'(x_0, x_1)^h$, we get that

$$z^p - z \;=\; x - tx_1^p + a^p x_1^p - ax_1 - dax_1^p \;=\; x - ax_1 + (a^p - da - t)x_1^p \;=\; x - ax_1 \;,$$

which shows that

$$x_1 \;\in\; L'(z) \;.$$

This in turn yields that $b \in L'(z)^h$ and consequently,

$$x_0 \;=\; z - ax_1 - b \in L'(z)^h \;.$$

Altogether, we have proved that

$$L'(x_0, x_1)^h \;=\; L'(z)^h$$

is henselian rational.

Let us discuss one more problem about the model theory of $\mathbb{F}_p((t))$ that becomes visible through our above example. It can be shown that for every $k \in \mathbb{N}$, the sentence

$$\forall X \exists X_0, \ldots, X_{p^k-1}, Y : \; X \;=\; X_0^{p^k} - X_0 + tX_1^{p^k} + \ldots + t^{p^k-1}X_{p^k-1}^{p^k} + Y \;\wedge\; vY \geq 0$$

holds in $\mathbb{F}_p((t))$ as well as in every maximal field which satisfies axiom system (5). On the other hand, given any $n \in \mathbb{N}$, the construction of (L, v) can be modified in such a way that for some k the above sentence does not hold in (L, v) and that the smallest extension of (L, v) within any maximal immediate extension in which that sentence holds is at least of transcendence degree n over L. This is in drastic contrast to the tame behaviour shown by tame fields:

If $(M|K,v)$ is an immediate extension, (M,v) is a tame field and K is relatively algebraically closed in M, then also (K,v) is a tame field.

(For a proof, see [Ku11].) This property of tame fields is used in an essential way in the proof of Theorem 7 in order to reduce to immediate extensions of transcendence degree 1 (so that Theorem 12 can be applied). Apparently, in the case of fields elementarily equivalent to $\mathbb{F}_p((t))$, we have to succeed without this tool.

For the construction of the field L, I needed a handy criterion for defectless fields. The following is proved in [Ku8]:

Theorem 18 *A valued field of positive characteristic is henselian and defectless if and only if it is separable-algebraically maximal and inseparably defectless.*

The proof uses a classification of Artin-Schreier extensions with non-trivial defect according to whether they can be obtained as a deformation of a purely inseparable extension with non-trivial defect, or not (cf. [Ku8]). This classification is also of independent interest. For instance, S. D. Cutkosky and O. Piltant [Cu–Pi] give an example of a tower of two Artin-Schreier extensions with non-trivial defect of a rational function field in which a certain form of "relative resolution" fails. It would be interesting to know whether such properties depend on the classification. In [Ku6], valued rational function fields are constructed which allow an infinite tower of Artin-Schreier extensions with non-trivial defect, but it is not clear whether one can obtain both sorts of extensions. The classification may also be important for the characterization of all valued fields whose maximal immediate extensions are finite (cf. [V] for the background).

2.4 But what about extremality for all polynomials?

Let us come back to the question whether every maximal field is extremal. We know the answer in the case of discrete valued fields:

Theorem 19 *If (K,v) is a henselian defectless field with value group isomorphic to $\mathbb{Z}$, then (K,v) is extremal.*

In [Del], Delon deduced this from the work of Greenberg [Gre]. An elegant model theoretic proof was given by Ershov. The theorem implies that in particular, $(\mathbb{F}_p((t)),v_t)$ is extremal. It also implies that every henselian defectless field with value group isomorphic to $\mathbb{Z}$ is extremal with respect to all p-polynomials in several variables. An alternative proof for this fact can be found in [Dr–K]. It uses the local compactness of $\mathbb{F}_p((t))$. If this could be eliminated in the case of maximal fields, we could at least prove that every maximal field is extremal with respect to all p-polynomials in several variables. This generates the following question:

Open Problem 3 If a henselian field of characteristic $p>0$ is extremal with respect to all p-polynomials in several variables, does this imply that it is extremal?

Are p-polynomials representative for all polynomials when extremality is concerned? Theorem 16 indicates that modulo henselization this is true for polynomials in one variable. But can we associate directly to every polynomial in one variable a p-polynomial in one variable from which we can read off information about extremality? A result of Kaplansky ([Ka1], Lemma 10), originally proved to be used in the construction of one of the counterexamples to embeddability in power series fields, shows that this can be done over every henselian field with archimedean value group. Using technical machinery developed in [Ku1], this result can be generalized (the proof is implicit in [Ku1]):

Proposition 20 *Let (K, v) be a henselian field and $(a_\rho)_{\rho<\lambda}$ a pseudo Cauchy sequence in K without a limit in K. Pick a polynomial f of minimal degree such that the value $vf(a_\rho)$ is not ultimately fixed. Then there is an additive polynomial $\mathcal{A} \in K[X]$ such that for all large enough ρ,*

$$v(f(a_\rho) - \mathcal{A}(a_\rho)) > vf(a_\rho)$$

(which in particular implies that $vf(a_\rho) = v\mathcal{A}(a_\rho)$).

Open Problem 4 Is Proposition 20 also true for polynomials in several variables?

If this were not the case, then it would destroy our hope to capture the complete theory of $\mathbb{F}_p((t))$ by adjoining axioms about extremality with respect to additive polynomials to axiom system (5). That would mean that additive polynomials are important but do not tell us all the missing information about $\mathbb{F}_p((t))$.

It should be mentioned that the case of several variables is very much different from the case of one variable, and there is not much hope of treating it by induction on the number n of variables starting with $n = 1$. Indeed, if $(L|K, v)$ is an immediate extension generated by a polynomial f, then a pseudo Cauchy sequence of algebraic type can be constructed with respect to which the value of f is not fixed (for these notions, see [Ka1]). This has been done in [Er2] and in [Ku8]. A similar procedure is *not* known for the case of several variables.

2.5 Concluding remarks about valued $K[\varphi]$-modules

Van den Dries' question can be reformulated as: *Determine the model theory of valued $K[\varphi]$-modules.* What do we mean by a "valued module"? There are some notions of "valued module" in the literature, but as far as I know they do not cover the case we are interested in. Basically, one could define a "valued module" to be a module which also has the structure of a valued abelian group. But without any further assumptions on the compatibility between module structure and valuation, this would not lead us far. So we have to choose axioms for the compatibility that cover the case we are interested in. I have done this in [Ku2], but these axioms are not yet in a very satisfactory form. Although the structure of $K[\varphi]$-modules can be nasty when K is not perfect, there is still

the valuation on them and it appears that with an appropriate choice of axioms one can tame these modules. Indeed, a first answer to van den Dries' question was given by his student Thomas Rohwer who proved in his thesis [Roh] the following results:

Theorem 21 *The elementary theory of* $\mathbb{F}_p((t))$ *as an* $\mathbb{F}_p((t))[\varphi]$*-module with a predicate for* $\mathbb{F}_p[[t]]$ *is model complete. The elementary theory of* $\mathbb{F}_p((t))$ *as an* $\mathbb{F}_p(t)[\varphi]$*-module with a predicate for* $\mathbb{F}_p[[t]]$ *is decidable.*

It should be noted that Pheidas and Zahidi [Ph–Za] prove analogous results for $\mathbb{F}_p[t]$ as an $\mathbb{F}_p[t][\varphi]$-module.

Theorem 21 immediately leads to a number of questions:

Open Problem 5 What do Rohwer's results tell us about the model theory of the valued field $\mathbb{F}_p((t))$?

Open Problem 6 Does the elementary theory of $\mathbb{F}_p((t))$ as an $\mathbb{F}_p((t))[\varphi]$- or $\mathbb{F}_p(t)[\varphi]$-module admit quantifier elimination in some natural language?

Rohwer works with predicates V_i that are interpreted by the sets of all elements of value $\geq i$. This gives less information than a binary predicate $P(x, y)$ interpreted by $vx \leq vy$ ("valuation divisibility").

Open Problem 7 What are the model theoretic properties of the elementary theory of $\mathbb{F}_p((t))$ as a valued $\mathbb{F}_p((t))[\varphi]$- or $\mathbb{F}_p(t)[\varphi]$-module in a language which includes a binary predicate for valuation divisibility?

Open Problem 8 What is the structure of extensions of valued $K[\varphi]$-modules? Can one prove Ax–Kochen–Ershov principles for valued $K[\varphi]$-modules?

An important tool in the model theory of valued fields is Kaplansky's well known result that a valued field is maximal if and only if every pseudo Cauchy sequence in this field has a limit (cf. [Ka1]). One can ask the same question for other valued structures. In the case of valued modules with value-preserving scalar multiplication, the corresponding result is already in the literature. For the case of valued modules with the above mentioned axioms that cover the case of the valued $K[\varphi]$-module $\mathbb{F}_p((t))$, I proved the corresponding result in [Ku2]. Together with Rohwer's work, this seems to be a good start towards a comprehensive study of valued $K[\varphi]$-modules, including a full answer to van den Dries' question, but quite a bit of work remains to be done.

3 Characterization of additive polynomials

In this section we give the basic characterizations of additive polynomials and prove Theorem 1.

Lemma 22 *Take $f \in K[X]$ and consider the following polynomial in two variables:*

$$g(X,Y) \;:=\; f(X+Y) - f(X) - f(Y)\;. \tag{16}$$

If there is a subset A of cardinality at least $\deg f$ in some extension field of K such that g vanishes on $A \times A$, then f is additive and of the form (2).

Proof: Assume that there is a subset A of cardinality at least $\deg f$ in some extension field of K such that g vanishes on $A \times A$. Take L to be any extension field of K. By field amalgamation, we may assume that A is contained in an extension field L' of L. For all $c \in L'$, the polynomials $g(c,Y)$ and $g(X,c)$ are of lower degree than f. This follows from their Taylor expansion. Assume that there exists $c \in L$ such that $g(c,Y)$ is not identically 0. Since A has more than $\deg g(c,Y)$ many elements, it follows that there must be $a \in A$ such that $g(c,a) \neq 0$. Consequently, $g(X,a)$ is not identically 0. But since A has more than $\deg g(X,a)$ many elements, this contradicts the fact that $g(X,a)$ vanishes on A. This contradiction shows that $g(c,Y)$ is identically 0 for all $c \in L$. That is, g vanishes on $L \times L$. Since this holds for all extension fields L of K, we have proved that f is additive.

By what we have shown, $g(c,Y)$ vanishes identically for every c in any extension field of K. That means that the polynomial $g(X,Y) \in K(Y)[X]$ has infinitely many zeros. Hence, it must be identically 0. Write $f = d_n X^n + \ldots + d_0$. Then $g(X,Y)$ is the sum of the forms $d_j(X+Y)^j - d_j X^j - d_j Y^j$ of degree j, $1 \leq j \leq \deg f$. Since g is identically 0, the same must be true for each of these forms and thus for all $(X+Y)^j - X^j - Y^j$ for which $d_j \neq 0$. But $(X+Y)^j - X^j - Y^j \equiv 0$ can only hold if j is a power of the characteristic exponent of K. Hence, $d_j = 0$ if j is not a power of p. Setting $c_i := d_{p^i}$, we see that f is of the form (2). □

Proof of Theorem 1: Suppose that $f \in K[X]$ is additive. Then the polynomial g defined in (16) vanishes on every extension field L of K. Choosing L to be infinite and taking $A = L$, we obtain from the foregoing lemma that f is of the form (2).

Conversely, for every $i \in \mathbb{N}$, the mapping $x \mapsto x^{p^i}$ is a homomorphism on every field of characteristic exponent p. Hence, every polynomial $c_i X^{p^i}$ is additive, and so is the polynomial $\sum_{i=0}^{m} c_i X^{p^i}$. □

Corollary 23 *Take $f \in K[X]$.*
a) If f is additive, then the set of its roots in the algebraic closure $\tilde{K}$ of K is a subgroup of the additive group of $\tilde{K}$. Conversely, if the latter holds and f has no multiple roots, then f is additive.

b) If f satisfies condition (1) on a field with at least $\deg f$ many elements, then f is additive.

Proof: a): If f is additive and a, b are roots of f, then $f(a+b) = f(a) + f(b) = 0$; hence $a+b$ is also a root. Further, $f(0) = f(0+0) = f(0) + f(0)$ shows that $0 = f(0) = f(a-a) = f(a) + f(-a) = f(-a)$, so 0 and $-a$ are also roots. This shows that the set of roots of f form a subgroup of $(\tilde{K}, +)$.

Now assume that the set A of roots of f forms a subgroup of $(\tilde{K}, +)$, and that f has no multiple roots. The latter implies that A has exactly $\deg f$ many elements. Since $A + A = A$, the polynomial $g(X,Y) = f(X+Y) - f(X) - f(Y)$ vanishes on $A \times A$. Hence by Lemma 22, f is additive.

b): This is an immediate application of Lemma 22. □

Exercise 1 *a) Let K be any finite field. Give an example of a polynomial $f \in K[X]$ which is not additive but induces an additive mapping on $(K, +)$.*
b) Show that the second assertion in part a) of Corollary 23 fails if we drop the condition that f has no multiple roots. Replace this condition by a suitable condition on the multiplicity of the roots.
c) Deduce Corollary 23 from the theorem of Artin as cited in [L], VIII, §11, Theorem 18.

4 Rings of additive polynomials

This section is devoted to the structure of rings of additive polynomials. Euclidean division is discussed in the following

Proof of Theorem 2: Take $s = \sum_{i=0}^{m} c_i \varphi^i$ and $s' = \sum_{i=0}^{n} d_i \varphi^i$. If $\deg s' < \deg s$, then we set $q = 0$ and $r = s'$. Now assume that $\deg s' = n \geq m = \deg s$. Then

$$\deg(s' - d_n c_m^{-p^{n-m}} \varphi^{n-m} s) \leq n - 1 < \deg s' \, .$$

Now take $q \in K[\varphi]$ such that $\deg(s' - qs)$ is minimal. Then $\deg(s' - qs) < \deg s$. Otherwise, we could apply the above to $s' - qs$ in the place of s', finding some $q' \in R$ such that $\deg(s' - (q+q')s) = \deg(s' - qs - q's) < \deg(s' - qs)$ contradicting the minimality of q. Setting $r = s' - qs$, we obtain $s' = qs + r$ with $\deg r < \deg s$. We have proved that $K[\varphi]$ is left euclidean. If K is perfect, hence $K = K^{p^m}$, then we also have

$$\deg(s' - s\,(c_m^{-1} d_n)^{1/p^m} \varphi^{n-m}) \leq n - 1 < \deg s' \, ,$$

and in the same way as above one deduces that $K[\varphi]$ is right euclidean.

Now assume that K is not perfect and choose some element $c \in K$ not admitting a p-th root in K. Then $K^p \cap cK^p = \{0\}$ and

$$\varphi K[\varphi] \cap c\varphi K[\varphi] = \{0\}$$

since every nonzero additive polynomial in the set $\varphi K[\varphi]$ has coefficients in K^p whereas every nonzero additive polynomial in $c\varphi K[\varphi]$ has coefficients in cK^p. □

Remark 24 Let us state some further properties of the ring $K[\varphi]$ which follow from Theorem 2. More generally, let R be any left principal ideal domain. Then R is a left free ideal ring (fir), and it is thus a semifir, i.e., every finitely generated left or right ideal is free of unique rank (note that this property is left-right symmetrical, cf. [C2], Chapter 1, Theorem 1.1). Consequently, every finitely generated submodule of a (left or right) free R-module is again free, cf. [C2], Chapter 1, Theorem 1.1 . On the other hand, every finitely generated torsion free (left or right) R-module is embeddable in a (finitely generated) free R-module if and only if R is right Ore, cf. [C2], Chapter 0, Corollary 9.5 and [Ge], Proposition 4.1 . Being a semifir, R is right Ore if and only if it is a right Bezout ring. But if R is not right Ore, then it contains free right ideals of arbitrary finite or countable rank, and R is thus not right noetherian, cf. [C2], Chapter 0, Proposition 8.9 and Corollary 8.10 . Every projective (left or right) R-module is free, cf. [C2], Chapter 1, Theorem 4.1 . A right R-module is flat if and only if it is torsion free, and a left R-module M is flat if and only if every finitely generated submodule of M is free, cf. [C2], Chapter 1, Corollary 4.7 and Proposition 4.5 . In view of the above, the latter is the case if and only if every finitely generated submodule of M is embeddable in a free R-module. Further, a left R-module M is flat if and only if for every $n \in \mathbb{N}$ and all right linearly independent elements $r_1, \ldots, r_n \in R$,

$$\forall x_1, \ldots, x_n \in M: \ \sum r_i x_i = 0 \ \Rightarrow \ \forall i: \ x_i = 0 \ ,$$

cf. [C1], Chapter 1, Lemma 4.3 . As a semifir, R is a coherent ring. Finally, since R is left Ore, it can be embedded in a skew field of left fractions, cf. [C2], Chapter 0, Corollary 8.7 .

Note that in particular, the above shows that all finitely generated torsion free (left or right) $K[\varphi]$-modules are free if and only if K is perfect, that is, $K[\varphi]$ is euclidean on both sides.

Exercise 2 *Describe the relation of the degree functions on $K[X]$ and $K[\varphi]$ via the correspondence (3), giving thereby a proof of $\deg rs = \deg r + \deg s$. Show that it also satisfies $\deg r + s \leq \max\{\deg r, \deg s\}$ with equality holding if $\deg r \neq \deg s$. Can it be transformed into a valuation?*

5 Frobenius-closed bases of function fields

In this section, we prove the existence of Frobenius-closed bases of algebraic function fields $F|K$ of transcendence degree 1, and exhibit the connection between their existence and the structure of F as a $K[\varphi]$-module (for arbitrary transcendence degree).

Take an arbitrary extension $F|K$ of fields of characteristic $p > 0$. Recall that a K-basis B of F is called **Frobenius-closed** if $B^p \subset B$, where $B^p = \{b^p \mid b \in B\} = \varphi B$. In [Ku9] we need Frobenius-closed bases because they have the following property:

Lemma 25 *Take a Frobenius-closed basis z_j, $j \in J$, of $F|K$. If the sum*

$$s = \sum_{i \in I} c_i z_i \,, \quad c_i \in K \,, \; I \subset J \text{ finite}$$

is a p-th power, then for every $i \in I$ with $c_i \neq 0$, the basis element z_i is a p-th power of a basis element.

Proof: Assume that

$$s = \left(\sum_{j \in J_0} {c_j}' z_j \right)^p \,, \quad {c_j}' \in K$$

where $J_0 \subset J$ is a finite index set. Then

$$\sum_{i \in I} c_i z_i = s = \sum_{j \in J_0} ({c_j}')^p z_j^p$$

where the elements z_j^p are also basis elements by hypothesis, which shows that every z_i which appears on the left hand side (i.e., $c_i \neq 0$) equals a p-th power z_j^p appearing on the right hand side. □

We will show the existence of Frobenius-closed bases for algebraic function fields of transcendence degree 1 over a perfect field of characteristic $p > 0$, provided that K is relatively algebraically closed in F. We first prove the following:

Lemma 26 *If F is an algebraic function field of transcendence degree 1 over an algebraically closed field K of arbitrary characteristic and q is an arbitrary natural number > 1, then there exists a basis of $F|K$ which is closed under q-th powers.*

If $F = K(x)$ is a rational function field, then our lemma follows from the **Partial Fraction Decomposition**: Every element $f \in F$ has a unique representation

$$f = c + \sum_{n>0} c_n x^n + \sum_{a \in K} \sum_{n>0} c_{a,n} \frac{1}{(x-a)^n}$$

where only finitely many of the coefficients $c, c_n, c_{a,n} \in K$ are nonzero. If we put

$$t_a = \frac{1}{x-a} \,, \quad t_\infty = x$$

then it follows that the elements

$$1, \; t_a^n \;\text{ with }\; a \in K \cup \{\infty\}, \; n \in \mathbb{N}$$

form a K-basis of F; this basis has the property that **every** power of a basis element is again a basis element.

For general function fields the Partial Fraction Decomposition remains true in a modified form (according to Helmut Hasse) that we shall describe now. At this point, we need the Riemann-Roch Theorem. In order to apply it, we have to introduce some notation. In what follows, we always assume that K is relatively algebraically closed in F. A **divisor** of $F|K$ is an element of the (multiplicatively written) free abelian group generated by all places of $F|K$. (By a place of $F|K$ we mean a place of F which is trivial on K, i.e., $P|_K = \mathrm{id}$. We identify equivalent places.) The places themselves are called **prime divisors**. A divisor may thus be written in the form

$$A = \prod_P P^{v_P A}$$

where the product is taken over all places of $F|K$ and the $v_P A$ are integers, only finitely many of them nonzero. The **degree of a non-trivial place** P of $F|K$, denoted by $\deg P$, is defined to be the degree $[FP : K]$ (which is finite since $F|K$ is an algebraic function field in one variable). Accordingly, the **degree of a divisor** A, denoted by $\deg A$, is defined to be the integer $\sum_P v_P A \cdot \deg P$. By the symbol "$v_P$" we will also denote the valuation on F which is associated with the place P. Following the notation of [F–Jr], we set

$$\mathcal{L}(A) \;:=\; \{f \in F \mid v_P f \geq -v_P A \text{ for all places } P \text{ of } F|K\}$$

is a K-vector space. Indeed, $0 \in \mathcal{L}(A)$ since $v_P 0 = \infty > -v_P A$ for all places P of $F|K$. Further, $v_P(K^\times) = \{0\}$, hence $\forall c \in K^\times : \; v_P(cf) = v_P f$ for all P, so $f \in \mathcal{L}(A)$ implies $cf \in \mathcal{L}(A)$. Finally, if $f, g \in \mathcal{L}(A)$, then $v_P(f-g) \geq \min\{v_P f, v_P g\} \geq -v_P A$ for all P, hence $f - g \in \mathcal{L}(A)$. We write

$$\dim A \;:=\; \dim_K \mathcal{L}(A)\;.$$

The divisor A determines bounds for the zero and pole orders of the algebraic functions in $\mathcal{L}(A)$. For example, if $A = P^n$ with n a natural number, then $f \in \mathcal{L}(A)$ if and only if f has no pole at all (in which case it is a constant function) or has a pole at P of pole order at most $n = v_P A$.

Theorem 27 (Riemann-Roch)
Let $F|K$ be an algebraic function field in one variable with K relatively algebraically closed in F. There exists a smallest non-negative integer g, called the genus of $F|K$, such that

$$\dim A \geq \deg A - g + 1$$

for all divisors A of $F|K$. Furthermore,

$$\dim A = \deg A - g + 1$$

whenever $\deg A > 2g - 2$.

For a proof, see [Deu].

Let P_∞ be a fixed place of $F|K$ and R^∞ the ring of all $f \in F$ which satisfy $v_P f \geq 0$ for every $P \neq P_\infty$. The following is an application of the Riemann-Roch Theorem:

Corollary 28 *For every $P \neq P_\infty$ there exists an element $t_P \in F$ such that*

$$\begin{aligned} v_P t_P &= -1 \\ v_Q t_P &\geq 0 \quad \textit{for} \;\; Q \neq P, P_\infty \, . \end{aligned}$$

Proof: If we choose $n \in \mathbb{N}$ as large as to satisfy $n \deg P_\infty > 2g-2$, then by the Riemann-Roch Theorem,

$$\dim(PP_\infty^n) = \deg P + n \deg P_\infty - g + 1 > n \deg P_\infty - g + 1 = \dim P_\infty^n \, .$$

Hence there is an element $t_P \in \mathcal{L}(PP_\infty^n) \backslash \mathcal{L}(P_\infty^n)$. This element has the required properties. □

We return to the proof of our lemma, assuming that K is algebraically closed. Hence, K is the residue field of every place P of $F|K$ (that is, $\deg P = 1$). Every t_P of the foregoing corollary is the inverse of a uniformizing parameter for P. Every $f \in F$ can be expanded P-adically with respect to such a uniformizing parameter, and the principal part appearing in this expansion has the form

$$h_P(f) = \sum_{n>0} c_{P,n} t_P^n \, ,$$

where only finitely many of the coefficients $c_{P,n} \in K$ are nonzero, namely $n \leq -v_P f$. By construction, t_P has only a single pole $\neq P_\infty$ and this pole is P; the same holds for $h_P(f)$ (if $h_P(f) \neq 0$). Consequently,

$$h = f - \sum_{P \neq P_\infty} h_P(f)$$

has no pole other than P_∞ and is thus an element of R^∞. We have shown that f has a unique representation

$$f = h + \sum_{P \neq P_\infty} \sum_{n>0} c_{P,n} t_P^n$$

with coefficients $c_{P,n} \in K$ and an element $h \in R^\infty$. This shows that the elements

$$t_P^n \;\; \text{with} \;\; P \neq P_\infty, \; n \in \mathbb{N}$$

form a K-basis of F modulo R^∞ which has the property that every power of a basis element is again a basis element.

Now it remains to show that R^∞ admits a basis which is closed under q-th powers. An integer $n \in \mathbb{N}$ is called **pole number** of P_∞ if there exists $t_n \in R^\infty$ such that $v_{P_\infty} t_n = -n$. Let $H_\infty \subseteq \mathbb{N}$ be the set of all pole numbers. Fixing a t_n for every $n \in H_\infty$, we get a K-basis

$$1,\ t_n \quad \text{with} \quad n \in H_\infty$$

of R^∞. To get a basis which is closed under q-th powers, we have to carry out our choice as follows:

Observe that H_∞ is closed under addition; in particular

$$qH_\infty \subset H_\infty\ .$$

For every $m \in H_\infty \setminus qH_\infty$ we choose an arbitrary element $t_m \in R^\infty$ with $v_{P_\infty} t_m = -m$. Every $n \in H_\infty$ can uniquely be written as

$$n = q^\nu m \quad \text{where} \quad \nu \geq 0 \quad \text{and} \quad m \in H_\infty \setminus qH_\infty\ .$$

Accordingly we put

$$t_n = t_m^{q^\nu}$$

which implies

$$v_{P_\infty} t_n = q^\nu \cdot v_{P_\infty} t_m = -q^\nu m = -n\ .$$

This construction produces a K-basis

$$1,\ t_m^{q^\nu} \quad \text{with} \quad m \in H_\infty \setminus qH_\infty,\ \nu \geq 0$$

of R^∞, which is closed under q-th powers. This concludes the proof of our lemma.

For the generalization of this lemma to perfect ground fields of characteristic $p > 0$ we have to choose $q = p$.

Proof of Theorem 10: We have to prove:

Let F be an algebraic function field of transcendence degree 1 over a perfect field K of characteristic $p > 0$. If K is relatively algebraically closed in F, then there exists a Frobenius-closed basis for $F|K$.

If K is not algebraically closed, we have to modify the proof of the previous lemma since not every place P of K has degree 1. (Such a modification is also necessary for the Partial Fraction Decomposition in $K(x)$ if K is not algebraically closed.) The modification reads as follows:

For every place P of $F|K$, let

$$d_P = \deg P = [FP : K]$$

be the degree of P. For every $P \neq P_\infty$ we choose elements $u_{P,i} \in R^\infty$, $1 \leq i \leq d_P$, such that their residues $u_{P,1}P, ..., u_{P,d_P}P$ form a K-basis of FP. We note that for every $\nu \geq 0$,

the p^ν-th powers $u_{P,i}^{p^\nu}$ of these elements have the same property: their P-residues also form a K-basis of FP since K is perfect.
We write every $n \in \mathbb{N}$ in the form

$$n = p^\nu m \quad \text{with} \quad m \in \mathbb{N},\ (p,m) = 1,\ \nu \geq 0$$

and observe that the elements

$$u_{P,i}^{p^\nu} t_P^n \quad \text{with} \quad P \neq P_\infty,\ n \in \mathbb{N},\ 1 \leq i \leq d_P$$

form a Frobenius-closed K-basis of F modulo R^∞.

It remains to construct a Frobenius-closed K-basis of R^∞. This is done as follows: We consider the K-vector spaces

$$\mathcal{L}_n = \mathcal{L}(P_\infty^n) = \{x \in F \mid v_{P_\infty} x \geq -n \text{ and } v_P(x) \geq 0 \text{ for } P \neq P_\infty\}\ .$$

By our assumption that K is relatively algebraically closed in F, we have $\mathcal{L}_0 = K$. Further,

$$R^\infty \ = \ \bigcup_{n \in \mathbb{N}} \mathcal{L}_n\ .$$

We set

$$d_{\infty,n} \ := \ \dim \mathcal{L}_n/\mathcal{L}_{n-1} \ \geq \ 0\ .$$

(Note that by the Riemann-Roch Theorem, $d_{\infty,n} = [FP_\infty : K]$ for large enough n; cf. the proof of the above corollary.) Now for $n = 1, 2, ...$ we shall choose successively basis elements $t_{n,i} \in \mathcal{L}_n$ modulo $\mathcal{L}_{n-1}$. Then the elements

$$1,\ t_{n,i} \quad \text{with} \quad n \in \mathbb{N},\ 1 \leq i \leq d_{\infty,n}$$

form a K-basis of R^∞. To obtain that this basis is Frobenius-closed, we organize our choice as follows:

If $n = pm$, the p-th powers $t_{m,i}^p \in \mathcal{L}_n$ are linearly independent modulo $\mathcal{L}_{p(m-1)}$ and even modulo $\mathcal{L}_{pm-1} = \mathcal{L}_{n-1}$. This fact follows from our hypothesis that K is perfect: the existence of nonzero elements $c_i \in K$ with $\sum c_i t_{m,i}^p \in \mathcal{L}_{pm-1}$, i.e., $v_{P_\infty} \sum c_i t_{m,i}^p > -pm$, would yield $v_{P_\infty} \sum c_i^{1/p} t_{m,i} > -m$, hence $\geq -m+1$, showing that $\sum c_i^{1/p} t_{m,i} \in \mathcal{L}_{m-1}$, which is a contradiction. In our choice of the elements $t_{n,i}$ we are thus free to take all the elements $t_{m,i}^p$ and to extend this set to a basis of $\mathcal{L}_n$ modulo $\mathcal{L}_{n-1}$ by arbitrary further elements, if necessary (for n large enough, the elements $t_{m,i}^p$ will already form such a basis). This procedure guarantees that the p-th power of every basis element $t_{m,i}$ is again a basis element, namely equal to $t_{pm,j}$ for suitable j. Hence a basis constructed in this way will be Frobenius-closed. □

Let $F|K$ be an arbitrary extension of fields of characteristic $p > 0$. Both F and K are $K[\varphi]$-modules, and so is the quotient module F/K. Suppose that F/K is a free

$K[\varphi]$-module. Then it admits a $K[\varphi]$-basis. Let $B_0 \subset F$ be a set of representatives for such a $K[\varphi]$-basis of F/K. It follows that

$$B = \bigcup_{n=0}^{\infty} B_0^{p^n} \cup \{1\} = \bigcup_{n=0}^{\infty} \varphi^n B_0 \cup \{1\}$$

is a set of generators of the K-vector space F. By our construction of B, every K-linear combination of elements of $B \setminus \{1\}$ may be viewed as a $K[\varphi]$-linear combination of elements of B_0. This shows that the elements of B are K-linearly independent, and B is thus a Frobenius-closed basis of $F|K$. Note that B_0 is the basis of a free $K[\varphi]$-submodule M of F which satisfies $F = M \oplus K$.

The converse to this procedure would mean to extract a $K[\varphi]$-basis B_0 from a Frobenius-closed K-basis B. But B_0 can only be found if for every element $b \in B \setminus \{1\}$ there is some element b_0 which is not a p-th power in F and such that $b = b_0^{p^n}$ for some $n \in \mathbb{N} \cup \{0\}$. This will hold if no element of $F \setminus K$ has a p^n-th root for every $n \in \mathbb{N}$.

Lemma 29 *If $F|K$ is an algebraic function field (of arbitrary transcendence degree), and if K is relatively algebraically closed in F, then no element of $F \setminus K$ has a p^n-th root for every $n \in \mathbb{N}$.*

Proof: Let $f \in F \setminus K$. Since K is relatively algebraically closed in F, we know that f is transcendental over K. So we may choose a transcendence basis $\mathcal{T}$ of $F|K$ containing f. We may choose a K-rational valuation v on the rational function field $K(\mathcal{T})$ such that the values of all elements in $\mathcal{T}$ are rationally independent (cf., e.g., [Ku7]). This yields that $vK(\mathcal{T}) = \bigoplus_{t \in \mathcal{T}} \mathbb{Z}vt$. In particular, vf is not divisible by p in $vK(\mathcal{T})$. Since $F|K(\mathcal{T})$ is finite, the same is true for $(vF : vK(\mathcal{T}))$ by the fundamental inequality (4). This yields that there is some $n \in \mathbb{N}$ such that vf is not divisible by p^n in vF. Hence, f does not admit a p^n-th root in F. □

This lemma shows that if $F|K$ is an algebraic function field with K relatively algebraically closed in F, admitting a Frobenius-closed basis B and if we let B_0 be the set of all elements in B which do not admit a p-th root in F, then we obtain $B = \bigcup_{n=0}^{\infty} B_0^{p^n} \cup \{1\}$. Since the elements of B are K-linearly independent, the elements of B_0 are $K[\varphi]$-linearly independent over K. Moreover, B_0 is a set of generators of the $K[\varphi]$-module F over K. Hence, the set B_0/K is a $K[\varphi]$-basis of F/K. We have thus proved:

Proposition 30 *Let $F|K$ be an algebraic function field (of arbitrary transcendence degree), and K relatively algebraically closed in F. Then F admits a Frobenius-closed K-basis if and only if F/K is a free $K[\varphi]$-module.*

This lemma shows that Theorem 10 implies Theorem 11.

Open Problem 9 Do Theorems 10 and 11 also hold for transcendence degree > 1?

Open Problem 10 Do Theorems 10 and 11 also hold if the assumption that K be perfect is replaced by the assumption that $F|K$ be separable? Note that if K is not perfect, then there exist places P of $F|K$ such that $FP|K$ is not separable, even if $F|K$ is separable. In this case, the construction of the proof of Theorem 10 breaks down and it cannot be expected that there is a Frobenius-closed K-basis of F which is as "natural" as the ones produced by that construction.

Exercise 3 *Show that F/K cannot be a free $K[\varphi]$-module if K is not relatively algebraically closed in F. Does there exist an algebraic field extension which admits a Frobenius-closed basis? Prove a suitable version of Proposition 30 which does not use the assumption that K be relatively algebraically closed in F.*

6 G-modules and group complements

In this section, we introduce some notions that we will need in the next section. Take any group G. For $\sigma \in G$, **conjugation by** σ means the automorphism

$$G \ni \tau \ \mapsto \ \tau^\sigma := \sigma^{-1}\tau\sigma \ .$$

Note that

$$\tau^{\sigma\rho} = \rho^{-1}\sigma^{-1}\tau\,\sigma\,\rho = \rho^{-1}(\tau^\sigma)\rho = (\tau^\sigma)^\rho \quad \text{for all } \tau,\sigma,\rho \in G \ . \tag{17}$$

Further, we set $\tau^{-\sigma} := (\tau^{-1})^\sigma$ (which indeed is the inverse of τ^σ). As usual, we set $M^\sigma = \{m^\sigma \mid m \in M\}$ for every subset $M \subset G$. A subgroup N is normal in G if and only if $N^\sigma = N$ for all $\sigma \in G$. We always have $G^\sigma = G$. Hence, if H is a **group complement** of the normal subgroup N in G, that is,

$$HN = G \quad \text{and} \quad H \cap N = \{1\} \ , \tag{18}$$

then so is every conjugate H^σ for $\sigma \in G$. Uniqueness up to conjugation would mean that these are the only group complements of N in G.

We shall now introduce two notions that will play an important role in Section 7. A **right G-module** is an arbitrary group N together with a mapping μ from G into the group of automorphisms of N such that $\mu(\sigma\rho) = \mu(\rho) \circ \mu(\sigma)$. For example, to every $\sigma \in G$ we may associate the conjugation by σ; in view of (17), this turns G into a right G-module. In this setting, a subgroup N of G is normal if and only if it is a G-submodule of G. A mapping ϕ from G into a G-module N is called a **twisted homomorphism** (or **crossed homomorphism**) if it satisfies

$$\phi(\sigma\rho) = \phi(\sigma)^\rho\phi(\rho) \quad \text{for all } \sigma,\rho \in G \ . \tag{19}$$

As for a usual homomorphism, also the kernel of a twisted homomorphism is a subgroup of G, but it may not be normal in G.

Let us assume that H is a group complement of the normal subgroup N in G. It follows from (18) that every element $\sigma \in G$ admits a unique representation

$$\sigma = \sigma_H \sigma_N \quad \text{with } \sigma_H \in H\,,\, \sigma_N \in N \tag{20}$$

Note that H is a system of representatives for the left cosets of G modulo N. Since $N \lhd G$, we have $HN = NH$, and H is also a system of representatives for the right cosets of G.

Now assume in addition that N is abelian. Then the scalar multiplication of the G-module N given by conjugation reads as

$$\sigma^\rho = \rho_N^{-1}(\rho_H^{-1}\sigma\rho_H)\rho_N = \rho_H^{-1}\sigma\rho_H = \sigma^{\rho_H} \quad \text{for all } \sigma \in N\,,\, \rho \in G \tag{21}$$

since ρ_N and $\rho_H^{-1}\sigma\rho_H$ are elements of N. According to (20) and (21) we write

$$\sigma\rho = \sigma_H\sigma_N\rho_H\rho_N = \sigma_H\rho_H\rho_H^{-1}\sigma_N\rho_H\rho_N = \sigma_H\rho_H\sigma_N^\rho\rho_N\,.$$

Hence, the projection $\sigma \mapsto \sigma_H$ onto the first factor in (20) is the canonical epimorphism from G onto H with kernel N. The other projection $\sigma \mapsto \sigma_N$ is a twisted homomorphism from G onto N, satisfying

$$(\sigma\rho)_N = \sigma_N^\rho\rho_N \quad \text{for all } \sigma, \rho \in G\,; \tag{22}$$

it induces the identity on N, and its kernel is H.

7 Field extensions generated by p-polynomials

In this section, let K be a field of characteristic $p > 0$. By a **Galois extension** we mean a normal and separable, but not necessarily finite algebraic extension. A field extension $L|K$ is called **p-elementary extension** if it is a finite Galois extension and its Galois group is an elementary-abelian p-group, that is, an abelian p-group in which every nonzero element has order p. In particular, $[L : K]$ is a power of p.

In this section, we will consider the following larger class of all extensions $L|K$ which satisfy the following condition:

$$\left.\begin{array}{l}\text{there exists a Galois extension } K'|K \text{ which is linearly disjoint from } L|K,\\ \text{such that } L.K'|K' \text{ is a } p\text{-elementary extension}\\ \text{and also } L.K'|K \text{ is a Galois extension.}\end{array}\right\} \tag{23}$$

From the linear disjointness it follows that $\operatorname{Gal} L.K'|L \simeq \operatorname{Gal} K'|K$ and that $[L : K] = [L.K' : K']$ which yields that $[L : K] = p^n$ for some natural number n. For a further investigation of this situation, we will use the following notation. We set

$$L' := L.K'$$

and define

- $G := \operatorname{Gal} L'|K$,
- $N := \operatorname{Gal} L'|K' \lhd G$,
- $H := \operatorname{Gal} L'|L \simeq \operatorname{Gal} K'|K \simeq G/N$.

The group N is abelian of order p^n. Since $K'|K$ is assumed to be a Galois extension, N is a normal subgroup of G. That is, N is a right G-module with scalar multiplication given by conjugation:

$$(\sigma, \tau) \;\mapsto\; \sigma^\tau = \tau^{-1}\sigma\tau \quad \text{for all } \sigma \in N\,,\, \tau \in G\,.$$

Since $L.K' = L'$ and $L \cap K' = K$, we have that $H \cap N = 1$ and $G = HN$, that is, H is a group complement for N in G. As we have seen in the last section, every element $\sigma \in G$ admits a unique representation (20). Since N is abelian, the scalar multiplication of the G-module N is given by (21). The projection $\sigma \mapsto \sigma_N$ is a twisted homomorphism from G onto N, satisfying (22); it induces the identity on N, and its kernel is H.

Lemma 31 *If $L|K$ satisfies condition (23) then w.l.o.g., the extension $K'|K$ may assumed to be finite (which yields that also $L'|K$ is finite).*

Proof: Suppose that $K'|K$ is an arbitrary algebraic extension such that (23) holds. Let $N_0 := \{\tau \in G \mid \forall \sigma_N \in N :\ \tau^{-1}\sigma_N\tau = \sigma_N\}$ be the subgroup of all automorphisms in G whose action on N is trivial (i.e., N_0 is the centralizer of N in G). Since N is abelian, it is contained in N_0 . Consequently, the fixed field K_0 of N_0 in L' is contained in K' (which is the fixed field of N in L' by definition of N). Since N is a normal subgroup of G, also its centralizer N_0 is a normal subgroup of G, showing that $K_0|K$ is a Galois extension. We set $H_0 := G/N_0$. By our choice of N_0 , the action of G on N induces an action of H_0 on N which is given by $\rho^{-1}\sigma_N\rho = \tau^{-1}\sigma_N\tau$ for $\rho = \tau N_0 \in H_0$. Consequently, H_0 must be finite, being a group of automorphisms of the finite group N. This proves that $K_0|K$ is a finite Galois extension with Galois group H_0 . Recall that it follows from (23) that also $L|K$ is finite.

We claim that $H \cap N_0$ is a normal subgroup of G. Let $\tau \in H \cap N_0$ and $\sigma \in G$; we want to show that $\tau^\sigma \in H \cap N_0$. Write $\sigma = \sigma_H\sigma_N$ according to (20). Then $\tau^\sigma = \sigma_N^{-1}(\sigma_H^{-1}\tau\sigma_H)\sigma_N$; since $\sigma_H \in H$ and $N_0 \lhd G$, we find that $\tau' := \sigma_H^{-1}\tau\sigma_H \in H \cap N_0$. In particular, τ' lies in the centralizer of N. In view of $\sigma_N \in N$ we obtain $\tau^\sigma = \sigma_N^{-1}\tau'\sigma_N = \sigma_N^{-1}\sigma_N\tau' = \tau' \in H \cap N_0$. We have proved that $H \cap N_0$ is a normal subgroup of G. With L_0 the fixed field of $H \cap N_0$ in L', we hence obtain a Galois extension $L_0|K$. Since $L_0 = L.K_0$, the extension $L_0|K$ is finite.

Finally, it remains to show that $\operatorname{Gal} L_0|K_0 \simeq \operatorname{Gal} L'|K'$ which also yields that $L_0|K_0$ is p-elementary. Observe that $HN_0 = G$ since it contains $HN = G$. Now we compute: $\operatorname{Gal} L_0|K_0 = \operatorname{Gal} L'|K_0 \,/\, \operatorname{Gal} L'|L_0 = N_0/(H \cap N_0) \simeq H.N_0/H = G/H \simeq N = \operatorname{Gal} L'|K'$. We have proved that condition (23) also holds with K_0 , L_0 in the place of K' , L'. □

In view of this lemma, we will assume in the sequel that all field extensions are finite.

Like N, also the additive group $(L',+)$ is a right G-module, the scalar multiplication given by

$$(a,\tau) \;\mapsto\; a^\tau := \tau^{-1}a \quad \text{for all } a \in L' \,,\; \tau \in G \,.$$

Let us show:

Lemma 32 *There is an embedding $\phi:\ N \longrightarrow (L',+)$ of right G-modules.*

Proof: By the Normal Basis Theorem (cf. [L]), the finite Galois extension $K'|K$ admits a normal basis. That is, there exists $b \in K'$ such that b^ρ, $\rho \in \mathrm{Gal}\, K'|K$, is a basis of K' over K. Since H is a set of representatives in G for $\mathrm{Gal}\, K'|K$, we may represent these conjugates as b^ρ, $\rho \in H$. Let $\psi:\ N \to (K,+)$ be any homomorphism of groups (there is always at least the trivial one), and set

$$\phi(\sigma_N) := \sum_{\rho\in H} \psi(\rho\sigma_N\rho^{-1})\, b^\rho \quad \text{for all } \sigma_N \in N \,. \tag{24}$$

Since ψ is a group homomorphism from N into $(L',+)$, the same is true for ϕ. Given $\tau \in G$, we write $\tau = \tau_H\tau_N$; then $b^{\rho\tau} = (b^{\rho\tau_H})^{\tau_N} = b^{\rho\tau_H}$ since $b^{\rho\tau_H} \in K'$ and $\tau_N \in N = \mathrm{Gal}\, L'|K'$. Observing also that $H = H\tau_H$ and using (21), we compute:

$$\begin{aligned}
\phi(\sigma_N)^\tau &= \sum_{\rho\in H} \psi(\rho\sigma_N\rho^{-1})\, b^{\rho\tau} \;=\; \sum_{\rho\in H} \psi(\rho\tau_H^{-1}\sigma_N(\rho\tau_H^{-1})^{-1})\, b^\rho \\
&= \sum_{\rho\in H} \psi(\rho\sigma_N^{\tau_H}\rho^{-1})\, b^\rho \;=\; \phi(\sigma_N^{\tau_H}) \;=\; \phi(\sigma_N^\tau)
\end{aligned}$$

which shows that ϕ is a homomorphism of right G-modules.

Now we have to choose ψ so well as to guarantee that ϕ becomes injective. If $\phi(\sigma_N) = 0$ then $\psi(\rho\sigma_N\rho^{-1}) = 0$ for all $\rho \in H$ since by our choice of b, the conjugates b^ρ, $\rho \in H$, are linearly independent over K. In particular, $\phi(\sigma_N) = 0$ implies $\psi(\sigma_N) = 0$. Hence, ϕ will be injective if we are able to choose ψ to be injective. This is done as follows. The elementary-abelian p-group N may be viewed as a finite-dimensional $\mathbb{F}_p$-vector space. If K is an infinite field (which by our general assumption has characteristic p), then it contains $\mathbb{F}_p$-vector spaces of arbitrary finite dimension; so there exists an embedding ψ of N into $(K,+)$. If K is a finite field, then all finite extensions of K are cyclic, their Galois groups being generated by a suitable power of the Frobenius φ; consequently, N must be cyclic. Since it is also elementary-abelian, N is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ which is the additive group of $\mathbb{F}_p \subset K$. Hence also in this case, N admits an embedding ψ into $(K,+)$. $\square$

By composition with ϕ, the twisted homomorphism $\sigma \mapsto \sigma_N$ is turned into a mapping $\sigma \mapsto \phi(\sigma_N)$ from G into $(L',+)$. We shall write $\phi(\sigma)$ instead of $\phi(\sigma_N)$, thereby considering

the G-module homomorphism $\phi : N \to (L', +)$ as being extended to $\phi : G \to (L', +)$. By construction, the latter has kernel H and is injective on N. Further, it satisfies $\phi(\sigma\tau) = \phi((\sigma\tau)_N) = \phi(\sigma_N^\tau \tau_N) = \phi(\sigma_N)^\tau + \phi(\tau_N) = \phi(\sigma)^\tau + \phi(\tau)$ showing that ϕ is a twisted homomorphism in the following sense:

$$\phi(\sigma\tau) = \phi(\sigma)^\tau + \phi(\tau) \quad \text{for all } \sigma, \tau \in G \, . \tag{25}$$

We claim that there exists an element $\vartheta \in L'$ such that

$$\vartheta^\tau = \vartheta + \phi(\tau) \quad \text{for all } \tau \in G \, . \tag{26}$$

Note that (26) determines ϑ up to addition of elements from K. (Indeed, ϑ' satisfies the same equation if and only if $(\vartheta - \vartheta')^\tau = \vartheta - \vartheta'$, i.e., if and only if $\vartheta - \vartheta' \in K$.)

The element ϑ can be constructed as follows. We choose an element $a \in L'$ such that the trace $s := \mathrm{Tr}_{L'|K}(a) = \sum_{\sigma \in G} \sigma a = \sum_{\sigma \in G} a^\sigma$ is not zero (we have seen in the foregoing proof that such an element exists: we could choose a to be the generator of a normal basis of $L'|K$; the linear independence will then force the trace to be nonzero). We set

$$\vartheta := -\frac{1}{s} \sum_{\sigma \in G} \phi(\sigma)\, a^\sigma \, . \tag{27}$$

Given $\tau \in G$, we have $G\tau = G$ and

$$1 = \frac{1}{s} \sum_{\sigma \in G} a^\sigma = \frac{1}{s} \sum_{\sigma \in G} a^{\sigma\tau}$$

which we use to compute

$$\begin{aligned} \vartheta^\tau &= -\frac{1}{s} \sum_{\sigma \in G} \phi(\sigma)^\tau a^{\sigma\tau} \;=\; -\frac{1}{s} \sum_{\sigma \in G} ((\phi(\sigma)^\tau + \phi(\tau)) a^{\sigma\tau} - \phi(\tau) a^{\sigma\tau}) \\ &= -\frac{1}{s} \sum_{\sigma \in G} \phi(\sigma\tau) a^{\sigma\tau} + \phi(\tau) \frac{1}{s} \sum_{\sigma \in G} a^{\sigma\tau} \\ &= -\frac{1}{s} \sum_{\sigma \in G} \phi(\sigma) a^\sigma + \phi(\tau) \frac{1}{s} \sum_{\sigma \in G} a^\sigma \;=\; \vartheta + \phi(\tau) \, . \end{aligned}$$

This proves that ϑ indeed satisfies (26).

Remark 33 The additive analogue of Hilbert's Satz 90 (cf. [L] or [J], chapter 1, section 15) says that $\mathrm{H}^1(G, (L', +)) = 0$. Since the twisted homomorphism $\phi : G \to (L', +)$ may be interpreted as a 1-cocycle, this implies that ϕ splits, which indicates the existence of ϑ. Replacing the twisted homomorphism ϕ by an arbitrary 1-cocycle in our above computation provides a proof of this additive analogue.

Since H is the kernel of ϕ, (26) yields that H is the group of all automorphisms of $L'|K$ which fix ϑ. Since on the other hand, by definition of $H = \operatorname{Gal} L'|L$ the fixed field of H in L' is L, we know from Galois theory that $L = K(\vartheta)$. Let us now compute the minimal polynomial f of ϑ over K. The group N may be viewed as a system of representatives for the left cosets of G modulo H. Consequently, the elements ϑ^τ, $\tau \in N$, are precisely all conjugates of ϑ over K. So

$$f(X) = \prod_{\tau \in N} (X - \vartheta^\tau) = \prod_{\tau \in N} (X - \vartheta - \phi(\tau)) = \mathcal{A}(X - \vartheta) \ ,$$

where

$$\mathcal{A}(X) := \prod_{\tau \in N} (X - \phi(\tau)) \ .$$

The roots of $\mathcal{A}$ form the additive group $\phi(N)$. Since we have chosen ϕ to be injective, we have $|\phi(N)| = |N| = \deg \mathcal{A}$. By part a) of Corollary 23 it follows that $\mathcal{A}$ is an additive polynomial. In particular,

$$f(X) = \mathcal{A}(X - \vartheta) = \mathcal{A}(X) - \mathcal{A}(\vartheta) \ .$$

Since $f(X) \in K[X]$, we have $\mathcal{A}(X) \in K[X]$ and $\mathcal{A}(\vartheta) \in K$. Since $\deg f = \deg \mathcal{A} = |N| = [L : K] = [K(\vartheta) : K]$, f is the minimal polynomial of ϑ over K.

We have proved:

Theorem 34 *Let $L|K$ be an extension which satisfies condition (23). Then there exist an additive polynomial $\mathcal{A}(X) \in K[X]$ and an element $\vartheta \in L$ such that $L = K(\vartheta)$ and $\mathcal{A}(X) - \mathcal{A}(\vartheta) \in K[X]$ is the minimal polynomial of ϑ over K.*

As an example, let us discuss an important special case. Let us assume that $L|K$ is a Galois extension of degree p. Then its Galois group is just $\mathbb{Z}/p\mathbb{Z}$, and the extension is thus p-elementary. In the above setting, we may then choose $K' = K$ which yields $L' = L$, $G = N = \mathbb{Z}/p\mathbb{Z}$ and $H = 1$. The embedding $\phi : \ N \longrightarrow (L', +)$ may be chosen "by hand" to be the most natural one: $N = \mathbb{Z}/p\mathbb{Z} = (\mathbb{F}_p, +) \subset (L', +)$. We obtain

$$\mathcal{A}(X) = \prod_{i \in \mathbb{F}_p} (X - i) = X^p - X$$

since the latter is the unique polynomial of degree p which vanishes on all elements of $\mathbb{F}_p$. The extension $L|K$ is thus generated by the root ϑ of the polynomial $f(X) = X^p - X - \mathcal{A}(\vartheta)$ which we call an **Artin-Schreier polynomial**. The extension $L|K$ is an Artin-Schreier extension. So we have shown:

Theorem 35 *Every Galois extension of degree p of a field of characteristic $p > 0$ is an Artin-Schreier extension.*

Inspired by this special case, we want to investigate whether we can get more information about the additive polynomial $\mathcal{A}$ if we strengthen the hypotheses. For instance, ϕ may be injective even if ψ is not. In our special case, $N = \mathbb{Z}/p\mathbb{Z}$ was an irreducible G-module, that is, it did not admit any proper nonzero G-submodule. But if N is an irreducible G-module, then every G-module homomorphism ϕ can only have kernel 0 or N, so if it does not vanish, then it is injective. For ϕ as defined in (24), we obtain $\phi \neq 0$ if $\psi \neq 0$. So it will suffice to take $\psi : \ N \to (\mathbb{F}_p\,, +)$ as a nonzero (additive) character; it exists since N is a non-trivial p-group. With this choice of ψ, we obtain

$$\phi(N) \subset \sum_{\rho \in H} \mathbb{F}_p\, b^\rho = \sum_{\rho \in H} \mathbb{F}_p\, \rho b\ .$$

Since the coefficients of the polynomial $\mathcal{A}$ are the elementary symmetric polynomials of the elements $\phi(\tau)$, $\tau \in N$, they lie in the ring $\mathbb{F}_p[\,\rho b \mid \rho \in H]$.

The condition that N be an irreducible G-module has turned out to be of certain importance. It is satisfied in the following special case:

Lemma 36 *Assume that $L|K$ is minimal with the property (23), that is, there is no proper non-trivial subextension with the same property. Then N is an irreducible G-module.*

Proof: Assume that M is a G-submodule of N, that is, M is a normal subgroup of G. Then HM is a subgroup of G containing H. In view of the unique representation (20), we have $HM = H$ if and only if $M = 1$ and $HM = G$ if and only if $M = N$. Note that the fixed field L_1' of M in L' is a Galois extension of K containing K'. Further, the fixed field L_1 of HM is contained in L, and it satisfies $L_1.K' = L_1'$ since $HM \cap N = M \cap N = M$. Consequently, also $L_1|K$ has property (23).

Suppose now that $L|K$ is minimal with the property (23). Then $L_1 = L$ or $L_1 = K$. Hence $HM = H$ or $HM = G$, that is, $M = 1$ or $M = N$, showing that the G-module N is irreducible. □

We summarize our preceding discussion in the following

Lemma 37 *Assume that $L|K$ is minimal with the property (23). If $K'|K$ is infinite, we may replace it by a suitable finite subextension. For every $b \in K'$ generating a normal basis of $K'|K$, and for every nonzero additive character $\psi : \ N \to (\mathbb{F}_p, +)$, the G-module homomorphism ϕ defined in (24) is injective. Moreover, the coefficients of the corresponding additive polynomial $\mathcal{A}(X)$ lie in the ring*

$$K \cap \mathbb{F}_p[\,\rho b \mid \rho \in H]\ .$$

Exercise 4 *Let* $\operatorname{char} K = p > 0$ *and $L|K$ be an Artin-Schreier extension and ϑ an* **Artin-Schreier generator** *of $L|K$, that is, $L = K(\vartheta)$ and $\vartheta^p - \vartheta \in K$. Show that all other Artin-Schreier generators of $L|K$ are of the form $i\vartheta + c$ with $i \in \{1, 2, \ldots, p-1\}$ and $c \in K$. Can something similar be said in the setting of Theorem 34? (Hint: use the uniqueness statement following equation (26)).*

8 Minimal purely wild extensions

This section is devoted to the proof of Theorem 13 which shows the important connection between purely wild (and in particular, immediate) extensions of henselian fields of positive characteristic and additive polynomials.

Before we continue, we put together several facts from ramification theory that can be found in [En], [N] and [Ku12] or can be deduced easily from other facts (exercise for the reader). For a field L, we denote by $\tilde{L}$ its algebraic closure and by $\operatorname{Gal} L$ the absolute Galois group $\operatorname{Gal} \tilde{L}|L$ of L. Recall that for a henselian field (K,v), K^r denotes the ramification field of the extension $(K^{\mathrm{sep}}|K,v)$.

Theorem 38 *Let (K,v) be a henselian field and p the characteristic exponent of Kv. Then the following assertions hold:*
a) $\operatorname{Gal} K^r$ is a normal subgroup of $\operatorname{Gal} K$ and $K^r|K$ is a Galois extension.
b) $\operatorname{Gal} K^r$ is a pro-p-group, so the separable-algebraic closure of K is a p-extension of K^r.
c) The value group vK^r consists of all elements in the ordered divisible hull of vK whose order modulo vK is prime to p. The residue field K^rv is the separable-algebraic closure of Kv.
d) If $vK^r = vK$ (we say that $K^r|K$ is **unramified***), then for every Galois subextension $K'|K$ of $K^r|K$, we have $\operatorname{Gal} K'|K \simeq \operatorname{Gal} K'v|Kv$.*
e) Every finite extension $(K_2|K_1,v)$, where $K \subseteq K_1 \subseteq K_2 \subseteq K^r$, is defectless.
f) If L is an algebraic extension of K, then $L^r = L.K^r$, and the extensions $(L^r|K^r,v)$ and $(L|K,v)$ have the same defect.
g) If (L,v) is an immediate henselian extension of (K,v), not necessarily algebraic, then $L^r = L.K^r$.

Let (K,v) be a henselian field which is not tame and thus admits purely wild extensions (see Theorem 14). Theorem 13 will follow from Theorem 34 if we are able to show that every minimal purely wild extension $L|K$ satisfies condition (23) which is the hypothesis the latter theorem. As a natural candidate for an extension $K'|K$ which is Galois and linearly disjoint from $L|K$, we can take the extension $K^r|K$. By part f) of Theorem 38 we know that $L.K^r = L^r$. We set

- $\mathcal{G} := \operatorname{Gal} K$,
- $\mathcal{N} := \operatorname{Gal} K^r$, which is a normal subgroup of $\mathcal{G}$ and a pro-p-group,
- $\mathcal{H} := \operatorname{Gal} L$, which is a maximal proper subgroup of $\mathcal{G}$ since $L|K$ is a minimal non-trivial extension, and which satisfies $\mathcal{N}.\mathcal{H} = \mathcal{G}$ since $K^r|K$ is linearly disjoint from $L|K$
- $\mathcal{D} := \mathcal{N} \cap \mathcal{H} = \operatorname{Gal} L.K^r = \operatorname{Gal} L^r$.

The next lemma examines this group theoretical situation.

Lemma 39 *Let $\mathcal{G}$ be a profinite group with maximal proper subgroup $\mathcal{H}$. Assume that the non-trivial pro-p-group $\mathcal{N}$ is a normal subgroup of $\mathcal{G}$ not contained in $\mathcal{H}$. Then $\mathcal{D} = \mathcal{N} \cap \mathcal{H}$*

is a normal subgroup of $\mathcal{G}$ and the finite factor group $\mathcal{N}/\mathcal{D}$ is an elementary-abelian p-group. Further, $\mathcal{N}/\mathcal{D}$ is an irreducible right $\mathcal{G}/\mathcal{D}$-module.

Proof: By the maximality of $\mathcal{H}$, we have $\mathcal{H}\mathcal{N} = \mathcal{G}$. Since $\mathcal{N} \not\subset \mathcal{H}$, we have that $\mathcal{D}$ is a proper subgroup of $\mathcal{N}$. Since every maximal proper subgroup of a profinite group is of finite index, we have that $(\mathcal{N} : \mathcal{D}) = (\mathcal{G} : \mathcal{H})$ is finite. Observe that $\mathcal{D}$ is **$\mathcal{H}$-invariant** (which means that $\mathcal{D}^\sigma = \mathcal{D}$ for every $\sigma \in \mathcal{H}$). This is true since $\mathcal{N} \lhd \mathcal{G}$ and $\mathcal{H}$ are $\mathcal{H}$-invariant. Assume that $\mathcal{E}$ is an $\mathcal{H}$-invariant subgroup of $\mathcal{N}$ containing $\mathcal{D}$. Then $\mathcal{H}\mathcal{E}$ is a subgroup of $\mathcal{G}$ containing $\mathcal{H}$. From the maximality of $\mathcal{H}$ it follows that either $\mathcal{H}\mathcal{E} = \mathcal{H}$ or $\mathcal{H}\mathcal{E} = \mathcal{G}$, whence either $\mathcal{E} = \mathcal{D}$ or $\mathcal{E} = \mathcal{N}$ (this argument is as in the proof of Lemma 36). We have proved that $\mathcal{D}$ is a maximal $\mathcal{H}$-invariant subgroup of $\mathcal{N}$.

Now let $\Phi(\mathcal{N})$ be the Frattini subgroup of $\mathcal{N}$, i.e., the intersection of all maximal open subgroups of $\mathcal{N}$. Since $\mathcal{D} \neq \mathcal{N}$, we can pick some maximal proper subgroup of $\mathcal{N}$ containing $\mathcal{D}$, and since it also contains $\Phi(\mathcal{N})$, it follows that $\mathcal{D}\Phi(\mathcal{N}) \neq \mathcal{N}$. Being a characteristic subgroup of $\mathcal{N}$, the Frattini subgroup $\Phi(\mathcal{N})$ is $\mathcal{H}$-invariant like $\mathcal{N}$. Consequently, also the group $\mathcal{D}\Phi(\mathcal{N})$ is $\mathcal{H}$-invariant. From the maximality of $\mathcal{D}$ we deduce that $\mathcal{D}\Phi(\mathcal{N}) = \mathcal{D}$, showing that

$$\Phi(\mathcal{N}) \subset \mathcal{D} \ .$$

On the other hand, the factor group $\mathcal{N}/\Phi(\mathcal{N})$ is a (possibly infinite dimensional) $\mathbb{F}_p$-vector space (cf. [R–Zal], part (b) of Lemma 2.8.7). In view of $\Phi(\mathcal{N}) \subset \mathcal{D}$, this yields that also $\mathcal{D}$ is a normal subgroup of $\mathcal{N}$ and that also $\mathcal{N}/\mathcal{D}$ is an elementary-abelian p-group. Since $\mathcal{D}$ is $\mathcal{H}$-invariant, $\mathcal{D} \lhd \mathcal{N}$ implies that

$$\mathcal{D} \lhd \mathcal{H}\mathcal{N} = \mathcal{G} \ .$$

As a normal subgroup of $\mathcal{G}$, $\mathcal{N}$ is a $\mathcal{G}$-module, and in view of $\mathcal{D} \lhd \mathcal{G}$ it follows that $\mathcal{N}/\mathcal{D}$ is a $\mathcal{G}/\mathcal{D}$-module. If it were reducible then there would exist a proper subgroup $\mathcal{E}$ of $\mathcal{N}$ such that $\mathcal{E}/\mathcal{D}$ is a non-trivial $\mathcal{G}/\mathcal{D}$-module. But then, $\mathcal{E}$ must be a normal subgroup of $\mathcal{G}$ properly containing $\mathcal{D}$; in particular, $\mathcal{E}$ would be a proper $\mathcal{H}$-invariant subgroup of $\mathcal{N}$, in contradiction to the maximality of $\mathcal{D}$. □

This lemma shows that $L^r|K$ is Galois and $L^r = L.K^r$ is a finite p-elementary extension of K^r. Hence $L|K$ satisfies (23) with $K' = K^r$. We apply Theorem 34 to obtain an additive polynomial $\mathcal{A}(X) \in K[X]$ and an element $\vartheta \in L$ such that $L = K(\vartheta)$ and that $\mathcal{A}(X) - \mathcal{A}(\vartheta)$ is the minimal polynomial of ϑ over K. Since $L|K$ is a minimal purely wild extension by our assumption, it is in particular minimal with property (23) and thus satisfies the hypothesis of Lemma 37. Hence, the extension $K^r|K$ can be replaced by a finite subextension $K'|K$, and $\mathcal{A}(X)$ may be chosen such that its coefficients lie in the ring $K \cap \mathbb{F}_p[\,\rho b \mid \rho \in H]$, where b is the generator of a normal basis of $K'|K$. Since vK is cofinal in $v\tilde{K} = \widetilde{vK}$, we may choose some $c \in K$ such that $vcb \geq 0$. Since (K, v) is henselian by assumption, it follows that $v\sigma(cb) = vcb \geq 0$ for all $\sigma \in \operatorname{Gal} K$. On the other

hand, cb is still the generator of a normal basis of $K'|K$. So we may replace b by cb, which yields that $K \cap \mathbb{F}_p[\,\rho b \mid \rho \in H] \subset \mathcal{O}_K$ and consequently, that $\mathcal{A}(X) \in \mathcal{O}_K[X]$.

Now assume in addition that $(K|k, v)$ is an immediate extension of henselian fields. Then we may infer from part g) of Theorem 38 that $K^r = k^r.K$. So the Galois extension K' of K is the compositum of K with a suitable Galois extension k' of k. In this case, b may be chosen to be already the generator of a normal basis of k' over k; it will then also be the generator of a normal basis of K' over K. With this choice of b, we obtain that the ring $K \cap \mathbb{F}_p[\,\rho b \mid \rho \in H]$ is contained in $K \cap k' = k$, whence $\mathcal{A}(X) \in \mathcal{O}_k[X]$. Let us summarize what we have proved; the following theorem will imply Theorem 13.

Theorem 40 *Let (K, v) be a henselian field and $(L|K, v)$ a minimal purely wild extension. Then $L^r|K$ is a Galois extension and $L^r|K^r$ is a p-elementary extension. Hence, $L|K$ satisfies condition (23), and there exist an additive polynomial $\mathcal{A}(X) \in \mathcal{O}_K[X]$ and an element $\vartheta \in L$ such that $L = K(\vartheta)$ and that $\mathcal{A}(X) - \mathcal{A}(\vartheta)$ is the minimal polynomial of ϑ over K. If $(K|k, v)$ is an immediate extension of henselian fields, then $\mathcal{A}(X)$ may already be chosen in $\mathcal{O}_k[X]$.*

Let us conclude this section by discussing the following special case. Assume that the value group vK is divisible by all primes $q \neq p$. Then by part c) of Theorem 38, $K^r|K$ is an unramified extension. Consequently by part d) of Theorem 38, $\mathrm{Gal}\, K'|K \simeq \mathrm{Gal}\, \overline{K'}|\overline{K}$ and we may choose the element b such that $\overline{b}$ is the generator of a normal basis of $\overline{K'}|\overline{K}$. It follows that the residue mapping is injective on the ring $\mathbb{F}_p[\rho b \mid \rho \in H]$ and thus, also the mapping $\tau \mapsto \overline{\phi(\tau)}$ is injective. In this case, we obtain that

$$\overline{\mathcal{A}}(X) = \prod_{\tau \in N} (X - \overline{\phi(\tau)})$$

has no multiple roots and is thus separable.

9 p-closed fields

This section is devoted to the proofs of the two theorems that deal with p-closed fields of positive characteristic.

Proof of Theorem 5: We have to prove that

A field K is p-closed if and only if it does not admit any finite extensions of degree divisible by p.

"$\Leftarrow$": Assume that K does not admit any finite extensions of degree divisible by p. Take any p-polynomial $f \in K[X]$. Write $f = \mathcal{A} + c$ where $\mathcal{A} \in K[X]$ is an additive polynomial. Let h be an irreducible factor of f; by hypothesis, it has a degree d not divisible by p. Fix a root b of h in the algebraic closure $\tilde{K}$ of K. All roots of f are of the form $b + a_i$ where the a_is are roots of $\mathcal{A}$. By part a) of Corollary 23 the roots of $\mathcal{A}$ in $\tilde{K}$ form an additive

group. The sum of the roots of h lies in K. This gives us $db + s \in K$, where s is a sum of a subset of the a_is and is therefore again a root of $\mathcal{A}$. Likewise, $d^{-1}s$ is a root of $\mathcal{A}$ (as d is not divisible by p, it is invertible in K). Then $b + d^{-1}s = d^{-1}(db + s)$ is a root of f, and it lies in K, as required.

"$\Rightarrow$": (This part of the proof is due to David Leep.) Assume that K is p-closed. Since K is perfect, it suffices to take a Galois extension $L|K$ of degree n and show that p does not divide n. By the normal basis theorem there is a basis $b_1, \ldots, b_n$ of $L|K$ where the b_is are the roots of some irreducible polynomial over K. Since they are linearly independent over K, their trace is non-zero. The elements

$$1, b_1, b_1^p, \ldots, b_1^{p^{n-1}}$$

are linearly dependent over K since $[L : K] = n$. Therefore there exist elements $d_0, \ldots, d_{n-1}, e \in K$ such that the p-polynomial

$$f(X) \;=\; d_{n-1}X^{p^{n-1}} + \ldots + d_0X + e$$

has b_1 as a root. It follows that all the b_is are roots of f. Thus the elements $b_2 - b_1, \ldots, b_n - b_1$ are roots of the additive polynomial $f(X) - e$. Since these $n - 1$ roots are linearly independent over K, they are also linearly independent over the prime field $\mathbb{F}_p$. This implies that the additive group G generated by the elements $b_2 - b_1, \ldots, b_n - b_1$ contains p^{n-1} distinct elements, which therefore must be precisely the roots of $f(X) - e$. So $G + b_1$ is the set of roots of f. By hypothesis, one of these roots lies in K; call it ϑ. There exist integers $m_2, \ldots, m_n$ such that

$$\vartheta \;=\; m_2(b_2 - b_1) + \ldots + m_n(b_n - b_1) + b_1\,.$$

In this equation take the trace from L to K. The elements $b_1, \ldots, b_n$ all have the same trace; hence the trace of every $m_i(b_i - b_1)$ is 0. It follows that the trace $n\vartheta$ of ϑ is equal to the trace of b_1; as we have remarked already, this trace is non-zero. Hence $n\vartheta \neq 0$, which shows that n is not divisible by p. □

Proof of Theorem 6: We have to prove:

A henselian valued field of characteristic $p > 0$ is p-closed if and only if it is an algebraically maximal Kaplansky field.

We will use Theorem 5 throughout the proof without further mention. Assume first that (K, v) is henselian and that K is p-closed. Since every finite extension of the residue field Kv can be lifted to an extension of K of the same degree, it follows that Kv is p-closed. Likewise, if the value group vK were not p-divisible, then K would admit an extension of degree p; this shows that vK is p-divisible. We have thus proved that (K, v) is a Kaplansky field. Since the degree of every finite extension of K is prime to p, it follows that (K, v) is defectless, hence algebraically maximal.

For the converse, assume that (K, v) is an algebraically maximal Kaplansky field. Since the henselization is an immediate algebraic extension, it follows that (K, v) is henselian. By Theorem 14, there exists a field complement W of K^r in $\tilde{K}$. As vK is p-divisible and Kv is p-closed, hence perfect, the same theorem shows that W is an immediate extension of K. Hence $W = K$, which shows that $K^r = \tilde{K}$. So every finite extension $L|K$ is a subextension of $K^r|K$ and is therefore defectless; that is, $[L : K] = (vL : vK)[Lv : Kv]$. As the right hand side is not divisible by p, (K, v) being a Kaplansky field, we find that p does not divide $[L : K]$. By Theorem 5, this proves that K is p-closed. □

References

[B] Bourbaki, N.: *Commutative algebra*, Paris (1972)

[C1] Cohn, P. M.: *Free rings and their relations*, London Math. Soc. Monograph **2**, London (1971)

[C2] Cohn, P. M.: *Free rings and their relations*, second edition, London Math. Soc. Monograph **19**, London (1985)

[Cu–Pi] Cutkosky, S. D. – Piltant, O.: *Ramification of valuations*, Adv. in Math. **183** (2004), 1–79

[Del] Delon, F.: *Quelques propriétés des corps valués en théories des modèles*, Thèse Paris VII (1981)

[Deu] Deuring, M.: *Lectures on the theory of algebraic functions in one variable*, Springer LNM **314** (1972)

[Dr–Ku] van den Dries, L. – Kuhlmann, F.-V.: *Images of additive polynomials in $\mathbb{F}_q((t))$ have the optimal approximation property*, Can. Math. Bulletin **45** (2002), 71–79

[En] Endler, O.: *Valuation theory*, Springer, Berlin (1972)

[Ep] Epp, Helmut H. P.: *Eliminating Wild Ramification*, Inventiones Math. **19** (1973), 235–249

[Er1] Ershov, Yu. L.: *On the elementary theory of maximal valued fields III* (in Russian), Algebra i Logika **6**:3 (1967), 31–38

[Er2] Ershov, Yu. L.: *Multi-valued fields*, Kluwer, New York (2001)

[F–Jr] Fried, M. – Jarden, M.: Field Arithmetic, Springer, Berlin (1986)

[Ge] Gentile, E. R.: *On rings with a one-sided field of quotients*, Proc. AMS **11** (1960), 380–384

[Go] Goss, D.: *Basic Structures of Function Field Arithmetic* , Springer, Berlin (1998)

[Gra] Gravett, K. A. H.: *Note on a result of Krull*, Cambridge Philos. Soc. Proc. **52** (1956), 379

[Gre] Greenberg, M. J.: *Rational points in henselian discrete valuation rings*, Publ. Math. I.H.E.S. **31** (1967), 59–64

[H] Huppert, B.: *Endliche Gruppen I*, Springer, Berlin (1967)

[J] Jacobson, N.: *Lectures in abstract algebra, III. Theory of fields and Galois theory*, Springer Graduate Texts in Math., New York (1964)

[Ka1] Kaplansky, I.: *Maximal fields with valuations I*, Duke Math. J. **9** (1942), 303–321

[Ka2] Kaplansky, I.: *Selected papers and other writings*, Springer, New York (1995)

[Kr] Krull, W.: *Allgemeine Bewertungstheorie*, J. reine angew. Math. **167** (1931), 160–196

[Ku1] Kuhlmann, F.-V.: *Henselian function fields and tame fields*, extended version of Ph.D. thesis, Heidelberg (1990)

[Ku2] Kuhlmann, F.-V.: *Valuation theory of fields, abelian groups and modules*, Habilitation thesis, Heidelberg (1995)

[Ku3] Kuhlmann, F.–V.: *Valuation theoretic and model theoretic aspects of local uniformization*, in: Resolution of Singularities — A Research Textbook in Tribute to Oscar Zariski. Herwig Hauser, Joseph Lipman, Frans Oort, Adolfo Quiros (eds.), Progress in Mathematics Vol. **181**, Birkhäuser Verlag Basel (2000), 381-456

[Ku4] Kuhlmann, F.-V.: *Elementary properties of power series fields over finite fields*, J. Symb. Logic **66** (2001), 771–791

[Ku5] Kuhlmann, F.-V.: *A correction to Epp's paper "Elimination of wild ramification"*, Inventiones Math. **153** (2003), 679–681

[Ku6] Kuhlmann, F.-V.: *Value groups, residue fields and bad places of rational function fields*, Trans. Amer. Math. Soc. **356** (2004), 4559–4600

[Ku7] Kuhlmann, F.–V.: *Places of algebraic function fields in arbitrary characteristic*, Advances in Math. **188** (2004), 399–424

[Ku8] Kuhlmann, F.–V.: *A classification of Artin Schreier defect extensions and a characterization of defectless fields*, submitted

[Ku9] Kuhlmann, F.–V.: *Elimination of Ramification I: The Generalized Stability Theorem*, submitted

[Ku10] Kuhlmann, F.–V.: *Elimination of Ramification II: Henselian Rationality*, in preparation

[Ku11] Kuhlmann, F.–V.: *The model theory of tame valued fields*, in preparation

[Ku12] Kuhlmann, F.–V.: Book in preparation. Preliminary versions of several chapters available at:

`http://math.usask.ca/~fvk/Fvkbook.htm`

[Ku–Pa–Ro] Kuhlmann, F.-V. – Pank, M. – Roquette, P.: *Immediate and purely wild extensions of valued fields*, Manuscripta Math. **55** (1986), 39–67

[L] Lang, S.: *Algebra*, Addison-Wesley, New York (1965)

[N] Neukirch, J.: *Algebraic number theory*, Springer, Berlin (1999)

[O1] Ore, O.: *Theory of non-commutative polynomials*, Ann. Math. **34** (1933), 480–508

[O2] Ore, O.: *On a special class of polynomials*, Trans. Amer. Math. Soc. **35** (1933), 559–584

[Ph–Za] Pheidas, T. — Zahidi, K.: *Elimination theory for addition and the Frobenius map in polynomial rings*, J. Symb. Logic **69** (2004), 1006–1026

[Pop] Pop, F.: *Über die Structur der rein wilden Erweiterungen eines Körpers*, manuscript, Heidelbeg (1987)

[R–Za] Ribes, L. – Zalesskii, P.: *Profinite Groups*, Springer, Berlin (2000)

[Ri] Ribenboim, P.: *Théorie des valuations*, Les Presses de l'Université de Montréal, Montréal, 2nd ed. (1968)

[Roh] Rohwer, T.: *Valued difference fields as modules over twisted polynomial rings*, Ph.D. thesis, Urbana (2003). Available at:

`http://math.usask.ca/fvk/theses.htm`

[V] Vámos, P.: *Kaplansky fields and p-algebraically closed fields*, Comm. Alg. **27** (1999), 629–643

[Wa1] Warner, S.: *Nonuniqueness of immediate maximal extensions of a valuation*, Math. Scand. **56** (1985), 191–202

[Wa2] Warner, S.: *Topological fields*, Mathematics studies **157**, North Holland, Amsterdam (1989)

[Wh1] Whaples, G.: *Additive polynomials*, Duke Math. Journ. **21** (1954), 55–65

[Wh2] Whaples, G.: *Galois cohomology of additive polynomials and n-th power mappings of fields*, Duke Math. Journ. **24** (1957), 143–150

[Zi] Ziegler, M.: Die elementare Theorie der henselschen Körper, *Inaugural Dissertation*, Köln (1972)

Mathematical Sciences Group, University of Saskatchewan,
106 Wiggins Road, Saskatoon, Saskatchewan, Canada S7N 5E6
email: fvk@math.usask.ca